ZXSEC US
管理员手册

中兴通讯股份有限公司

ZXSEC US
管理员手册

资料版本　　20080605-R1.0

产品版本　　V1.0

策　　划　中兴通讯学院　文档开发部

编　　著　李林灵 刘为超 罗辉

审　　核　管习辉 贺欢庆 李涛

测　　试

*　*　*　*

中兴通讯股份有限公司

地址：深圳市高新技术产业园科技南路中兴通讯大厦

邮编：518057

技术支持网站：http://support.zte.com.cn

客户支持中心热线：（0755）26770800　　800-830-1118

传真：（0755）26770801

E-mail：doc@zte.com.cn

*　*　*　*

声　明

本产品符合关于环境保护和人身安全方面的设计要求，产品的存放、使用和弃置应遵照产品手册、相关合同或相关国法律、法规的要求进行。

由于产品和技术的不断更新、完善，本资料中的内容可能与实际产品不完全相符，敬请谅解。如需查询产品的更新情况，请联系当地办事处。

若需了解最新的资料信息，请访问网站 **http://support.zte.com.cn**

意见反馈表

为提高中兴通讯用户资料的质量，更好地为您服务，希望您在百忙之中提出您的建议和意见，并请传真至：0755-26772236，或邮寄至：深圳市高新技术产业园科技南路中兴通讯大厦中兴通讯学院文档开发部收，邮编：518057，邮箱：doc@zte.com.cn。对于有价值的建议和意见，我们将给予奖励。

资料名称	ZXSEC US 管理员手册					
产品版本	V1.0			资料版本	20080605-R1.0	
您单位安装该设备的时间						
为了能够及时与您联系，请填写以下有关您的信息						
姓名		单位名称				
邮编		单位地址				
电话			E-mail			
您对本资料的评价		好	较好	一般	较差	差
	总体满意					
	工作指导					
	查阅方便					
	内容正确					
	内容完整					
	结构合理					
	图表说明					
	通俗易懂					
您对本资料的改进建议		详细说明				
	内容结构					
	内容详细					
	内容深度					
	表达简洁					
	增加图形					
	增加实例					
	增加 FAQ					
	其　　他					
您对中兴通讯用户资料的其他建议						

前　言

手册说明

本手册是 ZXSEC US 管理员手册 MR5 版本。

内容介绍

描述本书主要内容，介绍各章重点，指导使用者有针对性地使用本书。

章名	概要
第1章　系统概述	**ZXSEC US ASIC** 加速多种威胁保护防火墙系统增强了网络的安全性，避免了网络资源的误用和滥用，帮助您更有效的使用通讯资源的同时不会降低网络的性能。
第2章　基于 web 的管理器	本章介绍有关 ZXSEC US 设备用户友好基于 web 管理器管理接口的功能。
第3章　系统状态	连接到基于 web 的管理器可以查看 **ZXSEC US** 设备的当前系统状态您可以查看当前系统的状态信息包括序列号、运行时间、US Service[TM] 许可证信息、系统资源使用率、警报信息以及统计表信息。
第4章　系统虚拟域	本章将对如何在 ZXSEC US 设备中配置并使用虚拟域，使 ZXSEC US 设备能够作为多个虚拟设备进行操作，对多个网络提供单独的防火墙与路由策略。
第5章　网络配置	设置系统网络是指怎样将 ZXSEC US 设备配置到网络中作为防火墙设备生效。基本的网络设置包括配置 ZXSEC US 设备的接口与您的网络连接，以及配置 ZXSEC US 的 DNS 设置。更多高级的配置包括在设备网络配置中添加 VLAN 子接口与区域。
第6章　使用 DHCP	本章是关于如何配置 ZXSEC US LAN 接口的内容描述。
第7章　系统配置	本章关于 ZXSEC US 设备几项非网络性功能配置的说明，如 HA（高可用性）、SNMP、替换信息、与 VDOM 操作。
第8章　系统管理员设置	本章是有关如何在 ZXSEC US 设备中设置管理员帐户的信息。
第9章　系统维护	本章是有关如何备份与恢复系统配置以及如何配置从 US SERVICE 中心获得自动更新的内容。
第10章　静态路由	本章就如何定义静态路由以及创建路由策略内容进行了说明。设置 ZXSEC US 设备的路由是指设置提供给 ZXSEC US 设备将数据包转发到一个特殊目的地的所需的信息。
第11章　动态路由	本章就如何对路由流量配置动态路由协议通过大型或复杂的网络的内容进行了阐述。
第12章　路由监控	本章就如何截取路由监控表的内容进行描述。该列表是用于显示 ZXSEC US 设备中路由表条目的。

章名	概要
第13章　防火墙策略	防火墙策略控制所有通过 ZXSEC US 设备的通信流量。添加防火墙策略控制 ZXSEC US 接口、区域以及 VLAN 子接口之间的连接与流量。
第14章　防火墙地址	您可以根据需要添加、编辑以及删除防火墙地址。防火墙地址将被添加到防火墙策略的源以及目标地址字段。
第15章　防火墙服务	设置服务识别防火墙接收或拒绝的通信会话类型。您可以在策略中添加任何预先定义的服务。
第16章　防火墙时间表	设置时间表控制激活与中止策略的时间。
第17章　防火墙虚拟 IP 地址配置	本章节是有关 ZXSEC US 虚拟 IP 地址、IP 地址池以及配置在防火墙策略中配置使用等功能。
第18章　保护内容表	使用保户内容表对防火墙策略控制的流量应用不同的保护设置。本章将对在 NAT/路由以及透明模式下怎样添加保护内容表进行描述。
第19章　VPN IPSEC	本章是有关通过 web 管理器界面配置通道模式以及基于路由（接口模式）互联网安全协议 VPN 选项的说明。
第20章　VPN PPTP	本章是有关通过 web 管理器界面配置通道模式以及基于路由（接口模式）互联网安全协议 VPN 选项的说明。
第21章　VPN SSL 设置	本章是有关通过基于 Web 的管理器配置 VPN 菜单项下 SSL 功能的描述。只有运行于 NAT/路由模式下的 ZXSEC US 设备支持 SSL VPN 功能。
第22章　VPN 证书	本章是有关通过基于 web 管理器如何操作并管理 X.509 安全证书的内容。
第23章　设置用户	本章就有关如何建立用户帐户、用户组以及外部验证服务器内容进行了说明。通过定义认证用户（或称为用户组）可以控制对网络资源的访问。
第24章　反病毒保护	当您创建防火墙保护文件时，进入反病毒保护菜单访问反病毒配置选项。
第25章　IPS（入侵防护保护）	ZXSEC US 入侵防护系统（IPS）将特征与异常入侵防护结合，降低了威胁的潜伏期，增强了设备的可靠性。创建防火墙保护内容列表同时可以配置 IPS 选项。
第26章　Web 过滤	本章围绕四个部分，web 过滤功能、web 过滤内容屏蔽、URL 过滤与 US Service web 过滤，相互补充提供对互联网用户最大的控制与保护。
第27章　反垃圾邮件	本章是有关如何配置内容保护列表项中垃圾邮件过滤功能。
第28章　/P2P & VoIP	IM/P2P&VoIP 菜单是有关即时通讯的用户管理工具以及网络中使用 IM，P2P 以及 VoIP 功能的状态说明。IM，P2P 与 VoIP 必须在活动的内容保护列表中启动才能够生效。
第29章　日志与报告	本章是有关如何启动日志记录功能、查看日志文件以及通过 web 管理器查看报告的内容描述。

版本更新说明

产品版本	资料版本	资料编号	更新说明
V1.0	20080605-R1.0	sjzl20081968	手册第一次发行

本书约定

介绍符号的约定、键盘操作约定、鼠标操作约定以及四类标志。

1. 符号约定

带尖括号“＜ ＞”表示键名、按钮名以及操作员从终端输入的信息；带方括号“［ ］”表示人机界面、菜单条、数据表和字段名等，多级菜单用“→”隔开。如［文件→新建→文件夹］多级菜单表示［文件］菜单下的［新建］子菜单下的［文件夹］菜单项。

2. 键盘操作约定

格式	意义
加尖括号的字符	表示键名、按钮名。如＜Enter＞、＜Tab＞、＜Backspace＞、＜a＞等分别表示回车、制表、退格、小写字母 a
＜键 1+键 2＞	表示在键盘上同时按下几个键。如＜Ctrl+Alt+A＞表示同时按下“Ctrl”、“Alt”、“A”这三个键
＜键 1，键 2＞	表示先按第一键，释放，再按第二键。如＜Alt，F＞表示先按＜Alt＞键，释放后，紧接着再按＜F＞键

3. 鼠标操作约定

格式	意义
单击	快速按下并释放鼠标的左键
双击	连续两次快速按下并释放鼠标的左键
右击	快速按下并释放鼠标的右键
拖动	按住鼠标的左键不放，移动鼠标

4. 标志

本书采用四个醒目标志来表示在操作过程中应该特别注意的地方。

注意、小心、警告、危险：提醒操作中应注意的事项。

目　录

图目录

第1章 系统概述

1.1 概述

描述

欢迎选择中兴通讯产品，构筑实时网络保护。

ZXSEC US ASIC 加速多种威胁保护防火墙系统增强了网络的安全性避免了网络资源的误用和滥用，帮助您更有效的使用通讯资源的同时不会降低网络的性能。

US 设备获得了 ICSA 认证的反病毒服务、防火墙、IP 安全认证、SSL-TLS、IPS、入侵检测与反间谍软件服务。

ZXSEC US 病毒防火墙致力于网络安全，且易于管理。设备功能齐备，包括：

- 应用层服务，例如病毒防护和入侵保护、垃圾邮件过滤、网页内容过滤、IM、P2P 以及 VoIP 过滤。
- 网络层服务，例如防火墙、入侵检测、IPSec 与 SSLVPN 以及流量控制等。
- 管理服务，例如用户验证、向日志设备发送日志记录与报告、设备管理设置、基于 web 以及 CLI 的安全管理访问以及 SNMP。

ZXSEC US 病毒防火墙应用了中兴通讯动态威胁防护系统，具有芯片设计、网络通信、安全防御及内容分析等方面诸多技术优势。

独特的基于 ASIC 的网络安全构架能实时进行网络内容和状态分析，并及时启动部署在网络边界的防护关键应用程序，随时对您的网络提供最有效的安全保护。

ZXSEC US 系列病毒防火墙对现有的网络安全方案做了整合与补充；例如基于主机的病毒防护，降低设备、管理与维护成本的同时支持新的应用程序与服务。

内容

本章内容如下：

1.2 该版本中的更新内容

内容

本节着重介绍 USOS v3.0 MR5 版本中新增加的功能特性。

- US Service 管理服务---该项新的服务可以提供对固件升级与配置文件备份的远程管理功能。
- 接口别名设置---如需要，每个接口可以设定一个具体的名称。例如，port4 可以设定为“总部”，那么该端口的重新设定的“总部”名称将在各种设置中显示。
- PKI 功能的加强---ZXSEC US 的 OS V3.0MR5 中加强了 PKI 功能，例如对本地证书建立最多 5 个组织性的设备字段。
- 支持第三方 USB 密钥----USOS3.0MR5 支持指定格式的第三方 USB 密钥。
- 基于 VDOM 的保护内容表设置---每个 VDOM 包含默认的保护内容表设置与反病毒文件模式。您也可以对每个 VDOM 添加不同的保护内容表以及定制默认的保护内容项。
- PIM-SIM 环境下的多播目的 NAT---该功能是新增的，用于支持 NAT 下的多播数据流，且可以将数据流的源和/或目标地址进行地址转换。
- 防火墙策略验证功能的加强---防火墙策略验证提供基于源 IP 地址与策略 ID 的验证查询功能。
- IPv6 IPSec---IPv6 IPSec 功能提供对 IPSec VPN 中安全 IPv6 流量的支持。
- SSL-VPN 组标签---可以对 SSL-VPN 用户组添加多个标签。
- 日志上传功能---配置有硬盘的 ZXSEC US 设备可以将日志上传到 USLA 设备。

1.3 关于 ZXSEC US 病毒防火墙

参数信息

参数名称	参数说明
ZXSEC US6710	ZXSEC US6710 设备可以提供大型企业与服务商所需的承载级别的性能与可靠性。该设备应用了多个 CPU 与 ASIC 芯片，能够提供最大达 26Gbps 的输出量，满足多数应用的需要。ZXSEC US6710 设备含有八个 10/100/1000 网络接口，两个 SFP 接口，还包括两个双重带宽与两个单倍带宽的 ASM 扩展模块。
ZXSEC US6010 设备	ZXSEC US6010 病毒防火墙为大型企业和服务商应用所要求的千兆性能可靠性提供较高性能需求。该设备应用了多个 CPU 与 ASIC 芯片技术能够提供 4Gbp 的输出，满足了绝大部分应用需要。US6010 设备还备有冗余电源，减少了单向故障包括负载平衡操作与冗余故障，不间断运行。ZXSEC US6010 的高性能、可靠性与易于管理特点使其成为网络管理服务的理想选择。
ZXSEC US2010 设备	ZXSEC US2010 安全系统是为大型企业与服务商提供的高性能的安全解决方案。 ZXSEC US2010 自动从中兴通讯公司的 US Service 订制服务获取最新的更新信息，24 小时不间断防护对抗最新的病毒，蠕虫，特洛伊木马程序与其它网络威胁。ZXSEC US2010 具有的弹性构架针对出现的 IM，P2P 或者 VOIP 技术，以及识别例如 spywear，网络钓鱼（phishing）以及域名系统中毒（Pharming）等方法作出最快的响应。
ZXSEC US2010A	ZXSEC US1800A 安全系统是为大型企业与服务商提供的高性能的安全解决方案。 ZXSEC US2010A 突出的特性在于两个额外的光纤端口，加强了识别小型数据包的性能。ZXSEC US2010A 还提供基于安全平台的危急安全检测功能，集可靠性、可用性、快速部署、低运行成本以及对已知与未知的异常网络攻击现象出色的侦破率于一体。
ZXSEC US1300 设备	ZXSEC US1300 病毒防火墙拥有较高的吞吐量，8 个以太网接口（其中四个用户可以自行定义），支持 VLAN，与虚拟域。ZXSEC US1300 通过 HA 高可用性的冗余备份特性提供了无单点故障的安全保护；是要求较高网络安全性能的大型企业的理想选择。

参数名称	参数说明
ZXSEC US900 设备	ZXSEC US900 设备能够提供大型企业与服务商所需的电信运营商级别的设备性能与运行的可靠性。ZXSEC US900 设备拥有 10 个网络连接包括一个 4 端口的 LAN 交换机）与不丢弃会话包的自动故障检测功能的高可用性功能。ZXSEC US900 的高度灵活性，可靠性与易于管理的特性正是大型企业所期待的。
ZXSEC US550 设备	ZXSEC US550 设备的性能，可用性以及可靠性迎合了企业级别的需求。ZXSEC US550 同样也支持高可用性群集以及包括在 HA 设备主从设备切换时不会丢弃会话，该设备是关键任务系统的理想选择。
ZXSEC US350 设备	ZXSEC US350 设备易于部署与管理，为 soho 以及子机构之间的应用提供了高附加值与可靠的性能。US 安装指南通过简单的步骤指导用户在几分钟之内运行设备。
ZXSEC US180 设备	ZXSEC US180 为小型办公室或家庭式办公室设计应用 ZXSEC US180 支持的高级的性能例如 802.1Q，虚拟域以及 RIP 与 OSPF 路由协议。
ZXSEC US120 设备	ZXSEC US120 设备设计用于远距离办公以及远程办公的用户提供实时的网络防护。这样的网络防护包括基于 web 的反病毒、web 与邮件内容过滤、防火墙、VPN、基于网络的入侵检测与防护与流量控制的结合。ZXSEC US120 整合了 PC 卡（也称 PCMCIA）以扩展其他的功能，包括基于 3G 无线带宽的 Type II PC 卡与基于 IEEE802.11b/g WIFI 带宽的 MiniPCI 卡。扩展的功能使用户可以在不需要固定互联网连接的情况下建立安全的 3G/WiFi 无线访问ZXSEC US120 同时还整合了 2 个端口的 FXO VOIP 卡，用户可以享用低成本的 VOIP 通信。
US120 设备	US120 设备设计用于远程办公以及零售店的用户。
ZXSEC US70 设备	ZXSEC US70 设备设计用于远距离工作用户以及小型的具有 10 到 50 个员工远程办公用户 ZXSEC US70 设备具有两个 WAN 接口用于与互联网的冗余连接。ZXSEC US70 设备还具有 3 个端口的交换机功能，用于内部网络的连接并支持与其他 ZXSEC US70 设备配置组成 HA 群集。

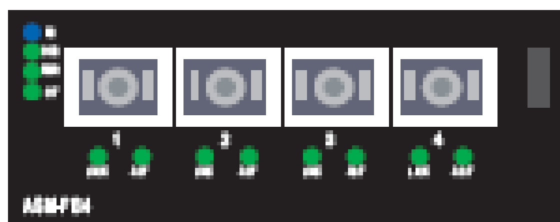


图1.3-1 USAMC 模块

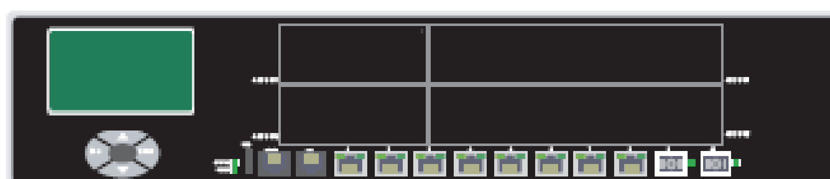


图1.3-2 ZXSEC US6710

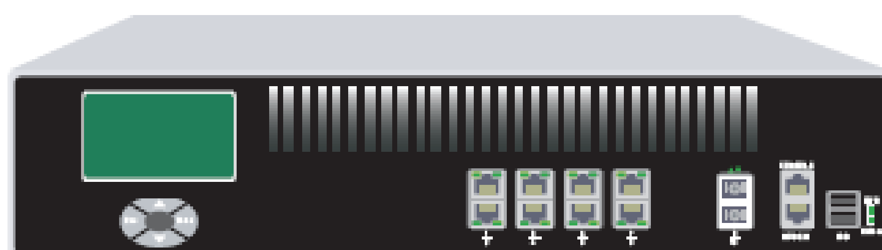


图1.3-3 ZXSEC US6010 设备



图1.3-4 ZXSEC US6010 设备

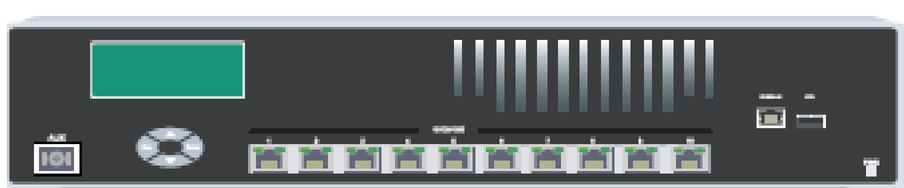


图1.3-5 ZXSEC US2010 设备

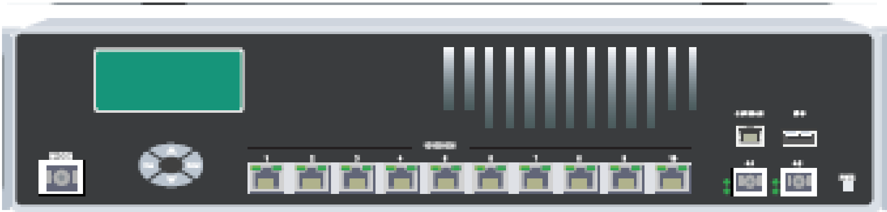


图1.3-6　ZXSEC US2010A

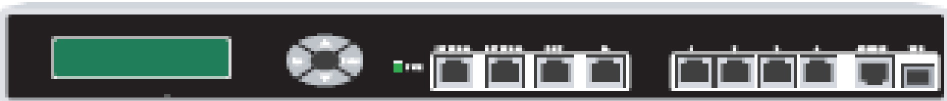


图1.3-7　ZXSEC US1300 设备



图1.3-8　ZXSEC US900 设备

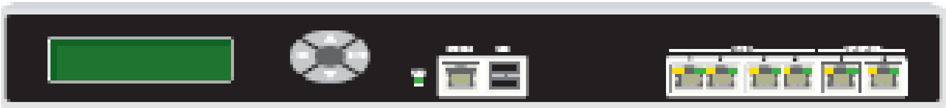


图1.3-9　ZXSEC US550 设备

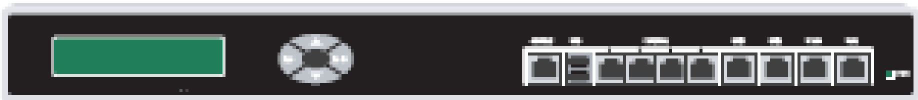


图1.3-10　ZXSEC US350 设备

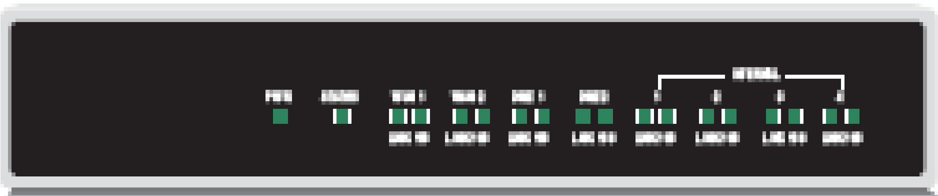


图1.3-11　ZXSEC US180 设备

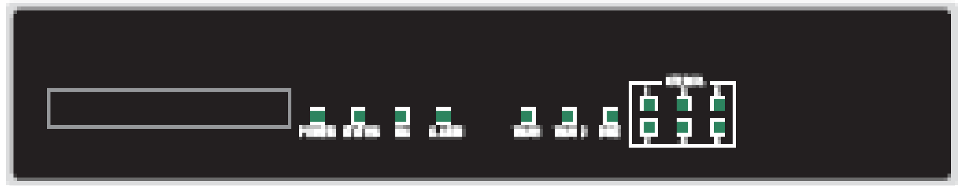


图1.3-12 ZXSEC US120 设备



图1.3-13 ZXSEC US70 设备

1.4 关于本手册

内容

ZXSEC US 设备 V3.0 MR5 管理员使用手册对如何 ZXSEC US 设备管理工具，基于 web 的管理器与命令行接口（CLI）；以及如何使用管理工具配置功能选项进行了详细说明。

本手册是按照基于 web 管理器界面菜单功能项的顺序而叙述的。手册开始首先说明与描述了 ZXSEC US 设备基于 web 的管理工具与虚拟域。接下来的章节中分别对基于 web 的管理器对应的系统管理菜单，路由器菜单，防火墙菜单，VPN 菜单都使用了单独的章节详细说明。其后，同样对用户、反病毒、入侵检测、网页过滤、反垃圾邮件、IM/P2P 与日志与报告均以单独的章节叙述。

该手册的最新版本可以在中兴通讯公司的网站中中兴通讯技术文档中获得。文中所叙述的信息也可以点击基于 web 管理器页面中在线帮助查看。

有关 ZXSEC US 的 OS V3.0 版本更为详细的信息，访问中兴通讯公司网站技术文档以及知识库。

该管理员使用手册包括以下章节：

- 基于 web 的管理器:介绍有关基于 web 管理器的功能,包括怎样注册 ZXSEC US 设备以及如何使用基于 web 管理器的在线帮助。
- 系统状态：有关系统状态页面以及 ZXSEC US 设备的面板。您可以查看设备状态信息，包括序列号、运行时间、US Service 许可证信息、系统资源使用率、警报信息以及统计表信息。本章还对用户可以更改的系统状态进

行了说明，包括更改设备固件，主机名称以及系统时间。

- 虚拟域

  介绍如何操作 ZXSEC US 设备的虚拟域，作为多个虚拟设备，对多个网络提供独立的防火墙与路由服务。

- 系统设置

  描述如何在 ZXSEC US 设备中配置物理接口、虚拟接口以及 DNS 设置。

- 系统 DHCP

  提供有关 ZXSEC US 设备作为 DHCP 服务器或 DHCP 中继代理时如何配置设备接口。

- DHCP：

  如何配置 ZXSEC US 接口作为 DHCP 服务器或 DHCP 中继代理。

- 系统配置

  有关配置 HA 与虚拟群集，配置 SNMP 以及替换信息以及更改操作模式的步骤。

- 系统管理

  通过添加与编辑管理员帐户定义系统管理员的访问权限，配置全局管理设置，例如语言显示，超时设置，以及 web 管理接口。

- 系统维护

  有关如何使用管理计算机或 USB 硬盘备份与存储系统配置，使用修改控制以及配置启动 US SERVICE 中心更新，以及输入许可证密钥增加虚拟域的最大使用数量。

- 静态路由

  描述有关如何定义静态路由与创建路由策略。

- 创建静态路由

  创建将数据包转发到除了出厂默认的网关以外的目标地址。

- 动态路由

  有关如何配置动态协议将数据包路由通过大型或复杂的网络。

- 路由监控

解释如何截取路由监控表，该表显示了 US 路由表中条目。

- 防火墙策略

  有关如何添加防火墙策略控制 ZXSEC US 设备接口、区域与 VLAN 子接口之间的连接与流量。

- 防火墙地址

  有关如何对防火墙策略配置地址与地址组。

- 防火墙服务

  有关可用的防火墙服务以及如何对防火墙策略配置服务组。

- 防火墙时间表

  有关如何配置防火墙策略的固定或循环时间表设置。

- 防火墙虚拟 IP

  有关如何配置并使用虚拟 IP 地址与 IP 池。

- 内容保护列表

  如何对防火墙策略配置保护内容表。

- VPN IPSEC

  有关通道模式以及通过基于 web 的管理器可用的基于路由(接口模式)的 Internet 协议安全性(IPSec)VPN 选项。

- VPN PPTP

  有关如何使用基于 web 的管理器为 PPTP 用户指定 IP 地址的范围。

- VPN SSL

  有关基本的 SSL VPN 设置的信息。

- VPN 证书

  如何管理 X.509 安全证书内容。

- 用户

  通过用户认证如何控制对网络资源的访问。

- 反病毒服务

  描述了当您创建了防火墙保护内容列表后如何启动反病毒服务选项。

- 入侵检测服务

  描述了在创建防火墙保护内容列表时如何配置入侵检测(IPS)选项。

- 网页过滤服务

  描述了在创建防火墙保护内容列表时如何配置网页过滤选项。

- 反垃圾邮件服务

  描述了在创建防火墙保护内容列表时如何配置反垃圾邮件选项。

- IM/P2P&VoIP

  描述在创建防火墙保护内容列表时如何配置 IM、P2P 以及 VoIP 选项。您可以查看 IM、P2P 以及 VoIP 统计表获得网络中协议使用的情况。

- 日志与报告

  对通过基于 web 的管理器如何启动日志记录，查看日志文件与查看基本的报告。

文档中的注释

以下是该手册中的注释：

- 在所举的例子中，私有 IP 地址既可以用做私有也可以是公共 IP 地址。
- 注意与警告标识中的提示较为重要的信息。

注意：

突出另外其它的有用信息。

警告：

对于可能造成意外的不良的结果包括数据丢失或者设备损害等命令或程序发出警告提示。

排版说明

以下是该安装手册中使用的排版说明：

排版说明	举例
菜单命令	进入 VPN>IPSEC>阶段 1 并点击”新建”.

键盘输入	在网关名称字段，键入远程 VPN 或用户（例如，Central_office_1）
代码范例	Config sys global Set ips-open enable end
CLI 命令句法	Config firewall policy edit id_integer set http_retry_count <retry_interer> set natip <address_ipv4mask> end
文档名称	*ZXSEC US* 设备管理员使用手册
源文件内容	<HTML><HEAD><TITLE>Firewall Authentication</TITLE></HEAD> <BODY><H4>You must authenticate to use this service.</H4>
程序输出	Welcome！
变量	<address_ipv4>

1.5 客户服务与技术支持

中兴通讯公司技术支持将确保您的 ZXSEC US 系统在您的网络中能够快速启动，轻松配置并能够可靠运行。

敬请访问中兴通讯技术支持网站 http://support.zte.com.cn 获知更多中兴通讯所提供的技术支持服务。

第2章 基于 web 的管理器

2.1 概述

描述

本章介绍有关 ZXSEC US 设备用户友好基于 web 管理器管理接口的功能。

通过运行 Internet 浏览器的任何计算机使用 HTTP 或一个安全的 HTTPS 连接，您便能够配置并管理 **ZXSEC US** 设备。基于 web 的管理器支持多种语言。配置 **ZXSEC US** 设备使其接受来自任何 ZXSEC US 设备接口的 HTTP 与 HTTPS 管理访问。


添加内容
日志流量
接口: port2
过去60分钟
过去24小时
过去30天
流入流量
流出流量
系统状态
序列号 US
持续运行时间 4 天 22 小时 59 分钟
系统日期 Tue May 27 08:14:13 2008 [更改]
HA状态 主动-主动 [配置]
集群名称 US-HA
集群成员 US20103607501242/US20103607501242(主)
软件版本 US2010 3.00-b0650(MR6) [升级]
US Desktop 版本 [升级]
运行模式 NAT [更改]
虚拟域 Disabled 禁用 [启动]
当前管理员 1 [细节]
许可证信息
支持合同 不能连接 [配置]
US Service升级
防病毒 不能连接 [配置]
AV特征值 8.631 (升级 2008-01-15) [升级]
扩展设置 0.000 (升级 2003-01-01)
入侵防御 不能连接 [配置]
IPS特征值 2.442 (升级 2007-11-08) [升级]
Web过滤 不能连接 [配置]
反垃圾邮件 不能连接 [配置]
管理服务 不能连接 [配置]
虚拟域
允许VDOMs 10
CLI 控制台 (未连接)
点击连接……
系统资源
CPU占用率 0%
内存占用率 15%
日志服务硬盘额度 0%
设备操作
日志服务
重启
关闭
恢复出厂值
警告信息窗口
2008-05-28 01:37:01 系统重启
2008-05-23 01:15:04 系统重启
2008-05-22 01:50:58 系统重启
2008-05-16 09:07:03 系统重启
2008-05-13 15:38:22 系统重启
统计数据 (自从 2008-05-28 01:37:10)
会话 24 当前会话 [细节]
内容归档
HTTP 0 访问的网址 [细节]
HTTPS 0 访问的网址 [细节]
邮件 0 发送的邮件 [细节]
0 接收的邮件
FTP 0 访问的网址 [细节]
0 上传的文件
0 下载的文件
IM 0 传输的文件 [细节]
0 聊天的会话
0 消息
攻击日志
防病毒 0 捕捉的病毒 [细节]
IPS 0 阻断的攻击 [细节]
垃圾邮件 0 检测到垃圾邮件 [细节]
Web 0 阻断的网址 [细节]

图2.1-1 基于 web 的管理器界面图

使用基于 web 的管理器可以配置大部分的 ZXSEC US 设置以及监控 ZXSEC US 设备的状态。使用基于 web 管理器进行的配置更改无需重新设置防火墙或中断服务便可以生效。配置完成后，可以保存设置作为备用。所保存的配置在任何时间都可以恢复。

有关连接基于 web 管理器的信息，参见设备安装手册中“连接到基于 web 的管理器”。

内容

本章内容如下：

2.2 按钮栏功能

内容

基于 web 管理器中右上角的按钮栏可以访问 ZXSEC US 设备几项重要的功能。



图2.2-1 基于 **web** 的管理器按钮栏

2.2.1 备份 ZXSEC US 设备配置

内容

点击“备份配置”按钮，备份 ZXSEC US 设备配置。您可以将设备配置备份到：

- 您所使用管理 ZXSEC US 设备的本地 PC。
- 管理工作站；可以是进入“系统设置>管理>集中管理”配置的 USM 设备或

US Service 管理服务。

- 如果您所操作的 ZXSEC US 设备中有 USB 接口，您可以连接到 USB 硬盘，将配置备份到 USB 硬盘中。

有关备份与恢复 ZXSEC US 设备配置的详细信息，参见“备份与恢复”章节。



图2.2-2　备份 ZXSEC US 设备配置（US Service 管理服务）

2.3 基于 web 管理器的页面

2.3.1 基于 web 的管理器界面图

内容

基于 web 的管理器界面由菜单栏与状态说明页面组成，许多菜单或页面都有相应的多个导航栏。当您点击一个菜单项目，如系统管理，系统菜单会扩展为一个子菜单。接着点击其中一个子菜单后，相关联的页面会在其对应的导航栏中显示。点击导航栏查看不同的页面内容。

该手册中所述步骤将指导您通过指定菜单项目打开到具体页面；子菜单与导航栏如下：

1. 进入系统>网络>接口



图2.3-1 部分基于 web 的管理器界面图

2.3.2 基于 web 管理器的菜单

内容

通过菜单，您可以访问 ZXSEC US 设备主要特征的配置选项。

系统 配置系统设备，如网络接口，虚拟域，DHCP 服务，时间与系统选项。

交换 交换模式只适用于 ZXSEC US350A。该菜单中可以配置安全的交换性能，包括交换-VLAN、端口隔离、生成树协议、QoS 设置、IGMP 监听与 802.1X 验证。

路由器 配置静态与动态路由。

防火墙 配置应用网络防护功能的防火墙策略与内容保护表以及配置虚拟 IP 地址与 IP 池。

用户 与防火墙策略结合配置用户帐户，使其接受用户验证。以及配置外部验证服务器。

VPN 配置 IPSec、SSL 与 PPTP 虚拟专用网络。

反病毒保护 配置反病毒保护设置。

IPS 配置入侵检测系统。

web 过滤配置网页内容过滤服务。

反垃圾邮件 配置垃圾邮件过滤服务。

IM/P2P&报告 配置监控即时消息通信、P2P 通信以及 VoIP 通信流量。

日志与报告　配置日志功能以及查看日志信息。

列表　　许多基于 web 的管理器的页面都是列表的形式显示的。网络接口，防火墙策略，管理员以及用户列表等。

删除图标

新建

名称	#条目	保护内容表	注释	
builtin-pattern	18			
builtin-pattern01	0			

编辑图标

图2.3-2　基于 **web** 管理器列表的示例

该列表显示每个项目的信息，使用页面最右栏中显示的图标可以对项目进行编辑。在列表中您可以点击删除图标移除该项条目，或点击编辑图标对项目进行修改。

点击“新建”后打开一个对话框可以添加并定义新的项目创建新项目的对话框类似于编辑现有的项目的页面。

2.3.3 在基于 web 的管理器菜单的列表项中添加过滤器

内容

以下基于 web 管理器的页面中包含多个较复杂的列表，您可以添加过滤器控制列表中显示的信息。

- 会话列表
- 防火墙策略列表
- IPSec VPN 监控器
- 入侵防护预定义特征列表
- 日志与访问控制列表

过滤器的设置对查询列表中显示信息的得以有效的控制。例如，您可以进入“系统>状态”，点击“会话”栏中的“详细信息”查看 ZXSEC US 设备当前所处理的通信会话。一台使用率很高的 ZXSEC US 设备可能要处理相当多的会话。如果您想查看某会话的详细信息，使用过滤器设置可以很快的锁定要查看的信息。例如，您想查看由具体一项防火墙策略处理的所有通信。您可以添加策略 ID 过滤器只显示特殊策略 ID 或策略 ID 范围的会话。

您可以点击各种过滤器的图标显示编辑过滤器的窗口。在编辑过滤器窗口，您可以点击任何栏目以过滤并配置该栏目的过滤器。您可以一个栏目或多个栏目添加过滤器。对设置过滤的栏目，显示为绿色，不设置的栏目显示为灰色。

1 / 1　清除所有的过滤条目

#	协议	源地址	源端口	目标地址	目标端口	策略ID	结束(秒)	
1	tcp	10.16.26.180	1794	10.16.13.53	443		36	
2	tcp	10.16.26.180	1792	10.16.13.53	443		36	
3	tcp	10.16.26.180	1806	10.16.13.53	443		87	
4	tcp	10.16.26.180	1804	10.16.13.53	443		87	
5	tcp	10.16.26.180	1810	10.16.13.53	443		88	
6	tcp	10.16.26.180	1796	10.16.13.53	443		19	

图2.3-3　举例入侵保护预定义特征列表

过滤设置显示所有包含字符串“apache”、日志设置启动的且动作设置为“丢弃”，严重性级别设置为高的特征。

过滤器设置在您闲置基于 web 管理器超时，或退出管理器，甚至重启 ZXSEC US 设备后仍然会保存设置。

根据各个栏目中显示的信息的类型可以使用不同的过滤器设置。所有的情况下，您可以通过设定过滤项显示与设定过滤器匹配的信息或点击“NOT”显示不匹配的信息。

对包含数字的项目栏设置过滤器如果栏目中包含数字(例如,IP 地址或防火墙 ID)，过滤设置可以是单个数字或数字范围。

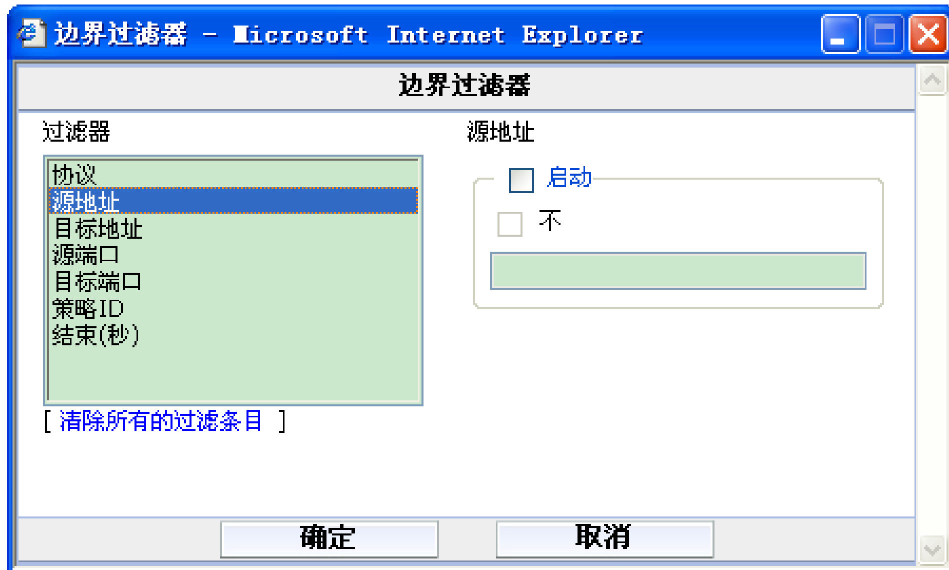


图2.3-4　会话列表过滤项设置显示源 IP 地址为 1.1.1.1 到 1.1.1.2 之间的会话

对包含文本字符串的项目栏设置过滤器

如果栏目中包含文本字符串（例如名称），您可以设置文本字符串过滤项。您可以设置与过滤项“文件字符串”精确匹配或包含所设定或不包含这些的信息显示。您也可以设定是否与所设定大写文本字符串的匹配的信息。

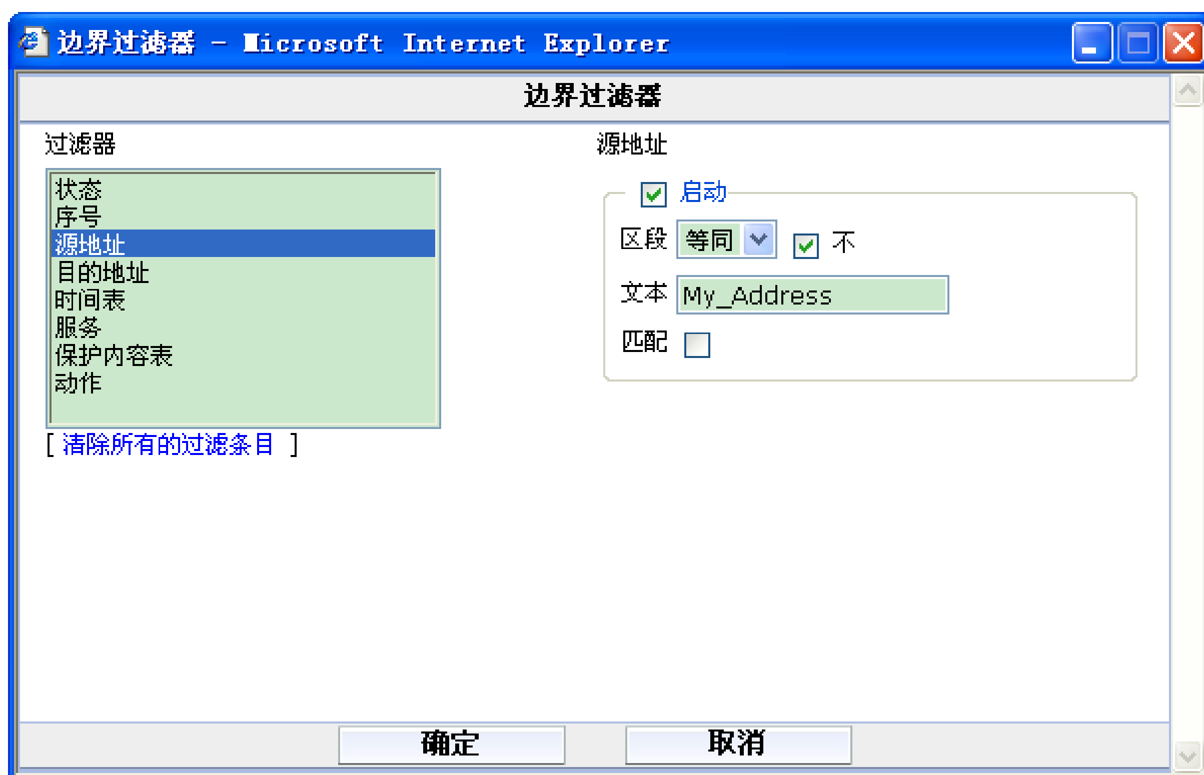


图2.3-5　防火墙策略列表过滤显示所有不包括源地址且名称为“my_address”的策略

对只包含具体条目的项目栏设置过滤器

对于那些只包含具体条目的项目栏（例如,日志信息严重性或预定义特征动作），可以从列表中选定单个的条目设置过滤项。这种情况下，您只能选定一个条目作为过滤项。

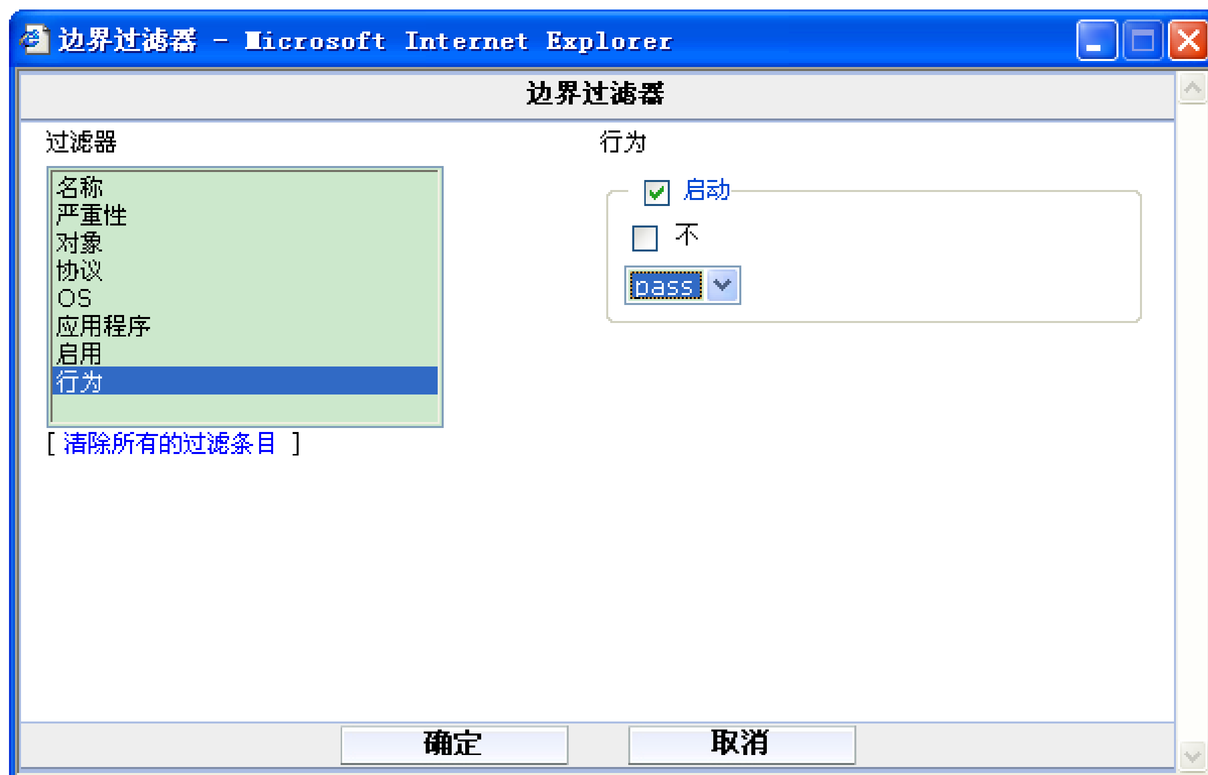


图2.3-6　IPS 预定义特征列表过滤显示所有“动作”设定为“重设”的特征

定制过滤器

其他用户定制的过滤项也是可用的。您可以根据日期时间范围来设定过滤日志信息。也可以设置日志信息级别过滤显示多个严重性级别的日志信息。

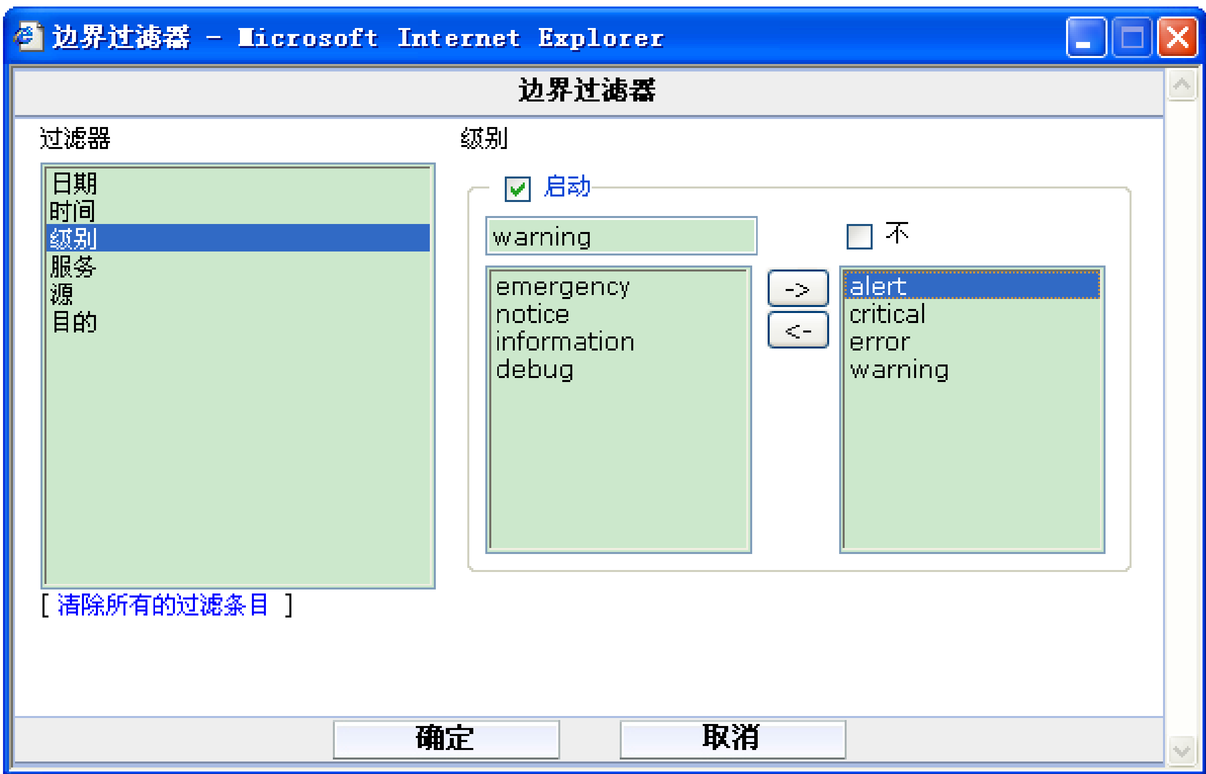


图2.3-7 设置日志访问过滤项显示所有日志级别为“警报”“错误”与“警告”的日志信息

定制过滤器

其他用户定制的过滤项也是可用的。您可以根据日期时间范围来设定过滤日志信息。也可以设置日志信息级别过滤显示多个严重性级别的日志信息。

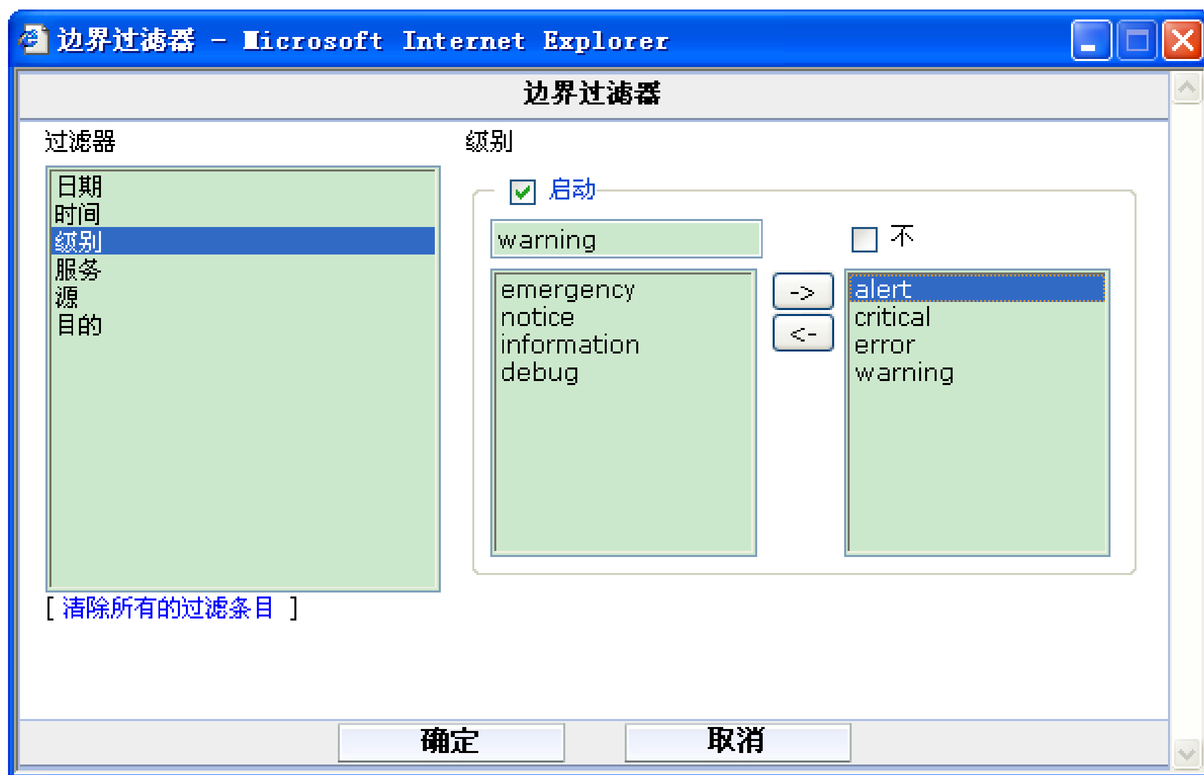


图2.3-8　设置日志访问过滤项显示所有日志级别为“警报”“错误”与“警告”的日志信息

图标

除了按键栏，基于 web 的管理器界面中还设有图标，点击这些图标也可以调用系统资源，执行操作任务。将鼠标停放在图标上将显示工具提示信息，便于您理解图标的功能特性。表 2 所列是基于 web 的管理器中的图标功能描述。

参数名称	参数说明
更改密码	更改管理员密码 该图标出现在管理员列表中，点击该图标您可以写入并修改 Admin 用户访问系统的密码
清除	清除一个日志文件
隐藏	点击隐藏一些字段。该图标应用在一些会话框及列表
设置栏	选择显示日志栏的格式
删除	删除一个项目。该图标出现在项目列表中,表示您可以对显示的项目进行删除
描述	描述列表的详细信息
下载	下载证书签发请求

参数名称	参数说明
下载或备份	下载日志文件或备份配置文件
编辑	编辑配置.该图标出现在列表的项目中，您可以点击该图标对项目进行编辑
扩展	点击扩展更多的字段。该图标应用在一些会话框及列表
过滤器	设置过滤选项。点击设定过滤项。该图标显示为绿色时,表示栏目设置了过滤，反之，呈灰色显示时，没有启动过滤。将鼠标停留在呈绿色显示的过滤器上，将显示具体设置的过滤细节
搜索	点击进行搜索
接入新的策略	创建一个新的策略代替当前的策略
移至	在列表中移动项目
下一页	查看当前列表的下一页
上一页	查看当前列表的上一页
刷新	点击更新页面信息
恢复设置	从文件中恢复配置
查看	查看配置 该图标出现在列表项中，如果您没有在该列表写入权限，将出现查看图标代替编辑图标

第3章 系统状态

3.1 概述

描述

连接到基于 web 的管理器可以查看 **ZXSEC US** 设备的当前系统状态您可以查看当前系统的状态信息包括序列号、运行时间、US Service[TM] 许可证信息、系统资源使用率、警报信息以及统计表信息。

注意：

查看系统状态页面时，浏览器必须支持 Java 脚本。

内容

本章内容如下：

3.2 系统状态

内容

查看系统状态页面，也就是系统面板，对照显示 **ZXSEC US** 设备当前的操作状态。所有具有读取访问系统配置权限的 **ZXSEC US** 管理员都可以查看系统状态信息。

当 ZXSEC US 设备作为一个 HA 群集的组成设备时,系统状态页面显示基本 HA 群集状态信息，包括群集名称、群集成员以及主设备名称。查看群集中所有设备的状态进入系统管理>配置>HA 并选择所要查看的群集中的成员设备详细信息，参见“HA 配置”。

具有对系统能够进行读取权限的 ZXSEC US 设备管理员可以更改或更新 ZXSEC US 设备信息。有关访问系统设置的详细信息，参见“访问系统设置”。

系统状态页面完全是可调节的。您可以点击选择显示的板块，以及每个板块在页面中放置的位置，您也可以将板块最大化或最小化。每个板块都有在最小化时便于识别的图标。

点击“添加内容”可以显示任何在当前的系统状态页面中没有显示的信息或者，点击“返回”恢复为默认的系统状态页面配置。

将鼠标停留在显示标题可以看到可选的显示选项。



图3.2-1　最小化后的显示项目

显示名称　　显示项的名称。

扩展箭头　　点击后最大或或最小化显示。

刷新　　点击后更新显示信息。

关闭　　点击后关闭显示。信息提示是否确认关闭。

3.3 更改系统信息

设备信息

系统状态	
序列号	US
持续运行时间	0 天 4 小时 22 分钟
系统日期	Wed May 28 05:59:20 2008 [更改]
HA状态	独立模式 [配置]
主机名	US20103607501242 [更改]
软件版本	US2010 3.00-b8746(MR6) [升级]
US Desktop版本	[升级]
运行模式	NAT [更改]
虚拟域	Disabled 禁用 [启动]
当前管理员	4 [细节]

图3.3-1 ZXSEC 设备信息

序列号 当前 ZXSEC US 设备的序列号。设备序列号是固有的，不随固件的升级而变化。

运行时间 ZXSEC US 设备在上一次启动后运行的时间。

系统日期 根据 ZXSEC US 设备的内部时钟记录的当前时间。点击“更改”，更改时间或配置 ZXSEC US 设备与 NTP 服务器同步时间。

主机名 当前运行的 ZXSEC US 设备主机名称。如果 ZXSEC US 设备当前运行于 HA 群集，该字段不显示信息。点击 “更改” ，更改主机名称。

群集名称 ZXSEC US 设备运行于 HA 群集显示每台群集成员设备的信息，包括主机名称、序列号、是主设备或是从属设备。如果该字段显示没有启动虚拟域，那么设备一定是运行于 HA 群集。

虚拟群集 1 设备分别在虚拟群集 1 与虚拟群集 2 中的角色。

虚拟群集 2 如果该字段显示没有启动虚拟域，那么设备一定是运行于 HA 群集。

软件版本 固件版本号。点击“更新”更改固件。

US Desktop 当前所装的 US Desktop 版本号。点击“更新”从管理计算机上传。

版本 新的 US Desktop 镜像到 ZXSEC US 设备。只有在 ZXSEC US 设备提供了从能够下载 US Desktop 软件的门户时，以上更新功能才能实现。

运行模式　当前 ZXSEC US 设备所运行的操作模式。除了 ZXSEC US350A 还可以运行于交换模式外，其他的 ZXSEC US 设备可以运行于 NAT 模式或透明模式。虚拟域同样也可以应用于 NAT 模式或透明模式。不同型号的 ZXSEC US 设备，可能该字段显示的信息不同。

虚拟域　ZXSEC US 设备中虚拟域的状态。点击“启动”或“撤消”更改虚拟域的状态。ZXSEC US350A 设备的交换机模式下不支持多个 VDOM 的操作更改虚拟域的状态将会终止管理员的会话，您需要重新登录。点击“更改”切换设备运行的模式。如果启动了虚拟域，该字段将显示当前虚拟去的操作模式。

当前管理员　当前登录 ZXSEC US 设备的管理员数量。点击“详情”查看关于每个管理员登录的详细信息，包括用户名、连接类型、连接的 IP 地址以及登录时间。

许可证信息

许可证信息显示 ZXSEC US 设备支持合同以及 US Service 订制的状态。ZXSEC US 设备通过连接的 US Service 网络自动更新许可证信息状态指示器。US Service 订制状态指示器呈绿色显示时表示连接正常，灰色显示时表示不能与 US Service 网络建立连接，黄色显示表示许可证过期。

点击任何配置选项将转到维护页面。

许可证信息

支持合同	不能连接 [配置]
US Service升级	
防病毒	不能连接 [配置]
AV特征值	8.631 (升级 2008-01-15) [升级]
扩展设置	0.000 (升级 2003-01-01)
入侵防御	不能连接 [配置]
IPS特征值	2.461 (升级 2008-01-18) [升级]
Web过滤	不能连接 [配置]
反垃圾邮件	不能连接 [配置]
虚拟域	
允许VDOMs	10

图3.3-2　许可证信息举例

支持合同　支持合同的编号以及过期时间。如果显示“请注册”，点击“请注册”先注册设备。

US Service

反病毒 US Service 反病毒许可证版本、发布日期与服务状态。如果许可证过期，点击“续订”更新许可证。

AV 定义 当前安装的反病毒定义版本。点击“更新”，手工更新定义。

入侵防护 US Service 入侵防护版本、发布日期与服务状态。如果许可证过期，点击“续订”更新许可证。

IPS 定义 当前安装的 IPS 定义版本。点击“更新”，手工更新定义。

Web 过滤 US Service Web 过滤许可证类型、过期日期与服务状态。如果许可证过期，点击“续订”更新许可证。

反垃圾邮件 US Service 反垃圾邮件许可证类型、过期日期与服务状态。如果许可证过期，点击“续订”更新许可证。

管理服务 US Service 管理服务许可证类型、过期日期与服务状态。

分析服务 US Service 日志与分析服务许可证类型、过期日期与服务状态。

服务帐户 ID 点击“更改”输入不同的服务帐户 ID。该 ID 用于识别您订制的服务。

虚拟域 ZXSEC US 设备支持的虚拟域数量。

警报信息 Console

USOS 中的一些命令只有通过 CLI 可以访问通过 telnet 或 SSH 使用第三方程序便可以连接到 CLI。

系统状态页面包括可用的 CLI console 访问。点击 Console，您可以自动从当前的 GUI 中登录到 CLI。CLI 的 console 默认的视窗不能改变大小或被移动。您可以从 CLI console 中拷贝粘贴文本信息。

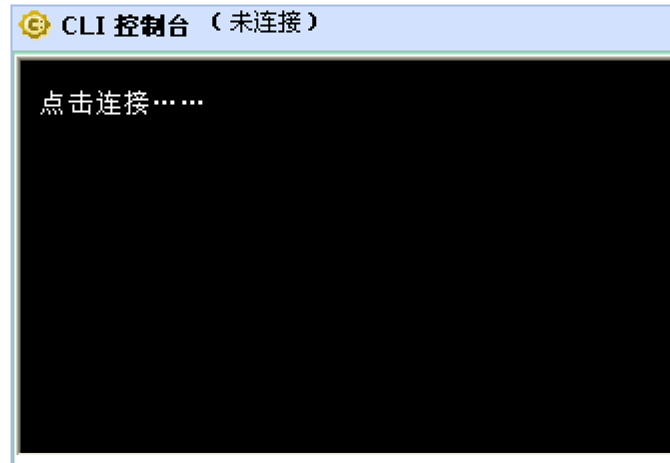


图3.3-3　CLI console

CLI console 窗口中有两个控制方法，自定义图标与分离控制。

点击“分离”控制，可以将 CLI Console 窗口从页面中剥离，改变视窗大小，再将窗口还原到页面。CLI console 从页面剥离后，可以点击“自定义”与“还原”。“还原”是指将剥离的 CLI 窗口重新返回到状态页面中。

点击“自定义”中的编辑图标，您可以设定 CLI 中文本文字显示的背景以及字体颜色。

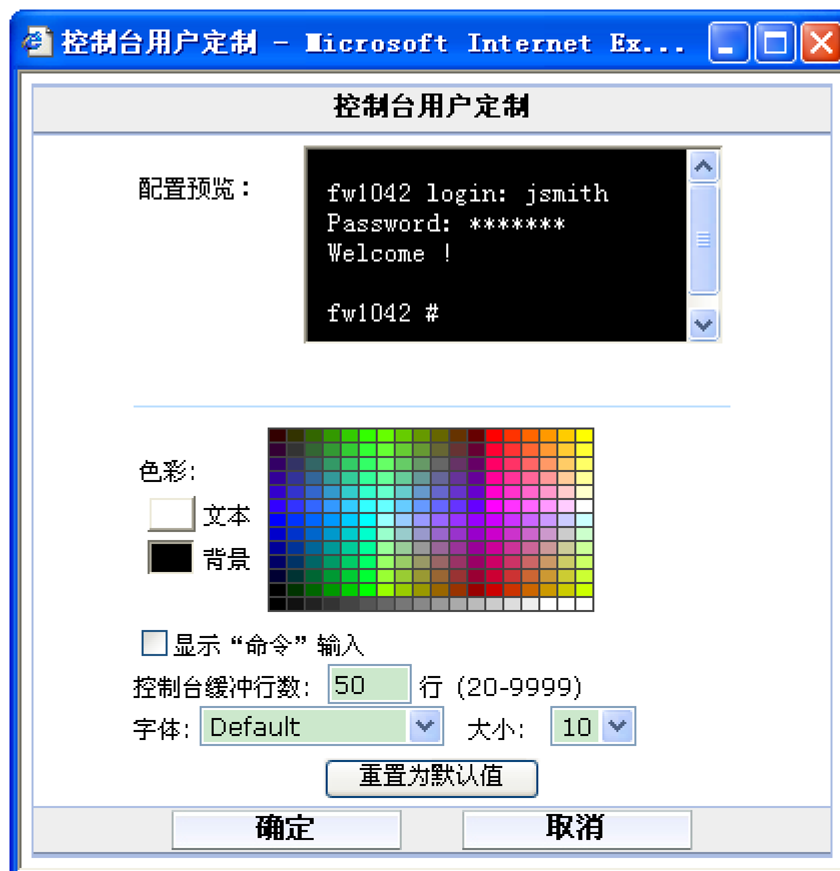


图3.3-4 自定义 CLI console 窗口

预览 预先查看设置更改。

文本 点击选择输入的 CLI 命令的字体颜色。

背景 设置 console 的背景色。

显示命令输入 点击允许外部输入。

控制台缓冲行数 设置内存中保持的 console 缓冲的行数。有效设定数值范围是 20 到 9999。

字体 设置字体。

大小 设定字号大小。默认的字号为 0。

重置为默认值 点击恢复为默认设置。

OK 点击保存设置更改并返回到 CLI console。

取消 点击取消设置更改并返回到 CLI console。

系统资源

任何状态页面中没有显示的系统资源，都可以点击“历史记录”图标进行查看。

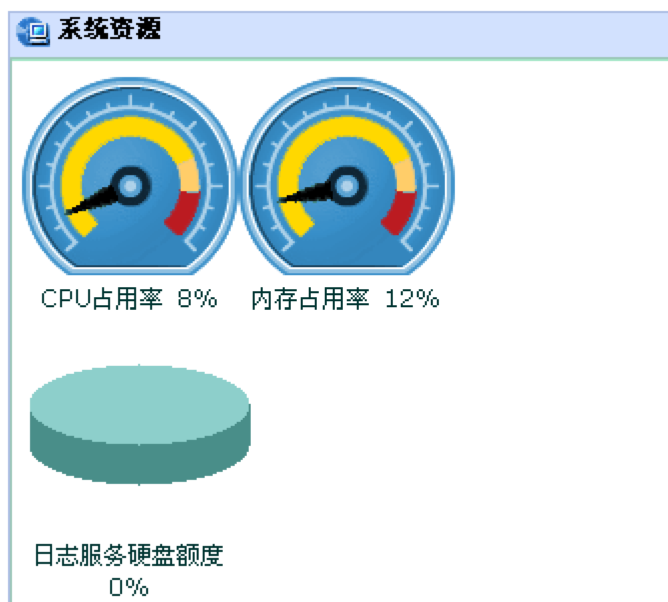


图3.3-5 系统资源

历史信息点击查看 CPU、内存、会话与网络的使用率。该页面还显示再最近 20 小时内病毒与入侵检测的信息。

CPU 占用率 当前 CPU 的使用情况。基于 web 的管理器显示核心进程的 CPU 使用情况。不包括管理进程的 CPU 占用情况（如与基于 web 的管理器的 HTTP 连接）。

硬盘的使用 如果ZXSEC US设备装有硬盘，显示当前硬盘的使用情况。基于web的管理器只显示核心进程的硬盘使用情况，不包括管理进程的硬盘使用情况（如与基于web的管理器的HTTP连接）。

USLA 硬盘配额 USLA 设备硬盘中 ZXSEC US 设备使用的配额，以饼状图加以百分比显示。该栏目只有在配置将日志记录到 USLA 设备时可用。

设备操作

ZXSEC US 设备的前面板显示设备以太网络接口的状态。如果接口呈绿色显示，表示已连接。将鼠标停顿在接口上，可以显示接口名称、IP 地址、掩码以及接口当前的状态。

点击“重新启动”或“关闭设备”将弹出窗口要求输入执行该操作的原因。所填写的原因将记录在“硬盘事件日志”中。硬盘事件日志需要使用 CLI 命令启动。同时需要启动事件日志与 Admin 日志。



图3.3-6 ZXSEC 设备接口状态（没有连接 USLA 设备）

INT/EXT/DMZ/HA/1/2/3/4 ZXSEC US 设备的以太网接口。这些接口数量与名称根据设备型号不同显示也不同。接口的状态是以接口的颜色显示来体现的，绿色表示已连接，灰色表示没有连接。将鼠标停留在接口，显示接口的配置与状态，包括接口全称、接口别称（如果进行了设定）、IP 地址与掩码、接口速率、接受与发送数据包的数量。如果您使用的 ZXSEC US 设备支持 ASM 模块且您安装的 ASM 中含有接口(例如，USASM-FB4 中有四个接口），这些接口将被添加到接口状态中显示。这些接口名称为 AMC/1，AMC/2 等等。

USLA ZXSEC US 设备与 USLA 外形镜像图之间的链接表示两个设备之间连接。红色“X”图标表示没有连接，绿色对勾表示设备之间已连接。

重启 点击关闭或重新启动设备系统将弹出对话框要求输入重新启动的原因，记录作为事件日志。

关闭 点击关闭设备。系统将弹出对话框要求输入重新启动的原因，记录作为事件日志。

恢复出厂值 点击将设备恢复为出厂默认设置系统弹出对话框确认信息。

警报信息 Console

根据警报信息可以跟踪 ZXSEC US 设备的设置更改情况。以下警报信息 Console 显示警报信息的类型：

警告信息窗口

- 2008-05-28 01:37:01 系统重启
- 2008-05-23 01:15:04 系统重启
- 2008-05-22 01:50:58 系统重启
- 2008-05-16 09:07:03 系统重启
- 2008-05-13 15:38:22 系统重启

图3.3-7　警报信息 Console 举例

警报信息 console 中可以显示以下类型的信息：

系统重启系统重新启动。出于操作人员的意愿或是电源开关跳闸致使的重启。

固件升级系统管理员进行的系统管理员在动态或非动态分区进行的升级。

固件降级　　系统管理员进行的系统管理员在动态或非动态分区进行的降级。

ZXSEC US 设备在 n 秒内达到了连接的极限　反病毒引擎在 n 秒内已经没有足够的内存可用了。这种条件下，根据设备型号或配置，数据包内容将被屏蔽的或未经过扫描就通过。

发现新的 USLA 设备与 USLA 设备失去连接　显示 ZXSEC US 发现新的 USLA 设备，或者 USLA 设备的连接。

每条信息中含有发布的时间与日期。如果没有足够的空间显示所有的信息，您可以点击“显示全部”查看剩余的信息。

点击“编辑”启动“用户定义警报信息”选项，您可以定义显示以下方面的警报信息。

- 重新启动系统信息
- 固件升级或降级信息
- 更改模式信息清除警报信息，点击“全部”在弹出的窗口选择“清除警报信息”。该操作将清除 ZXSEC US 设备中当前所有的警报信息。

统计信息

状态页面中的统计信息板块用于查看网络流量以及防护有关信息。

您可以快速查看 ZXSEC US 设备中流量的数量与类型以及任何试图进行的攻击。

需要查看某些信息的详细信息时，只需要点击对应信息的“详情”即可。

统计表中显示的信息可以被保存在日志文件中，这样的日志文件可以上传到 USLA 设备、本地进行保存或备份到外部网络资源中。利用日志信息数据，您可以查看网络活动的方向与趋势或某个时间段内发生的攻击以及相应的处理方法。

VDOM 模式下，系统状态页面中只可以查看全局配置下的统计信息。VDOM 配置下没有系统状态页面。系统状态页面中的内容存档与攻击日志统计信息只包括根 VDOM 的日志信息。该页面中不能查看非根 VDOM 统计表信息。

统计数据 (自从 2008-05-28 01:37:10)			
会话		164 当前会话	[细节]
内容归档			
	HTTP	0 访问的网址	[细节]
	HTTPS	0 访问的网址	[细节]
	邮件	0 发送的邮件	[细节]
		0 接收的邮件	
	FTP	0 访问的网址	[细节]
		0 上传的文件	
		0 下载的文件	
	IM	0 传输的文件	[细节]
		0 聊天的会话	
		0 消息	
攻击日志			
	防病毒	0 捕捉的病毒	[细节]
	IPS	0 阻断的攻击	[细节]
	垃圾邮件	0 检测到垃圾邮件	[细节]
	Web	0 阻断的网址	[细节]

图3.3-8 统计表信息举例

最近重启时间 ZXSEC US 设备重新启动时或重新恢复到出厂默认设置时该时间都将发生变化。距离 ZXSEC US 最近一次重启的时间（日，小时，秒）。

重设图标 点击将存档与攻击日志记录归零。

会话 ZXSEC US 设备处理的通信会话数量点击“详情”查看会话详细信息。

内容存档 通过 ZXSEC US 设备的 HTTP，邮件，FTP 与 IM/P2P 流量的摘要。“详情”页面列出所选类型的最近 64 个条目并提供到存储流量内容的 USLA 设备的链接。如果没有配置登录到 USLA 设备，“详情”页面所提供的链接将转到“日志与报告>日志配置>日志设置”页面。

攻击日志　　ZXSEC US 设备检测到的病毒、攻击、垃圾邮件信息与 URL 的摘要。“详情”页面提供最近 10 个条目，包括时间、源地址、目标地址以及其他信息。

更改设备信息

具有对系统配置读取权限的系统管理员可以更改系统时间、主机名称与 VDOM 的操作模式。

配置系统时间

1. 进入“系统>状态”。

2. 在系统信息栏，点击“系统时间线”项的“更改”按钮。

3. 选择时区并手工设置时间日期，或配置与 NTP 服务器同步。

时间设置
系统时间 Wed May 28 06:14:03 2008 刷新
时区选择 (GMT+8:00)Beijing,ChongQing,HongKong,Urumgi
夏时制
时间设置 时 6 分 14 秒 3
年 2008 月 May 日 28
与NTP服务器同步
服务器 pool.ntp.org
同步间隔 60 (1 - 1440 mins)
确定 取消

图3.3-9　时间设置

系统时间　　ZXSEC US 设备当前的系统时间。

刷新　　点击刷新显示当前的系统时间。

时区选择　　选择当前的系统时间所属的时区。

夏时制　设置系统根据夏令时制自动更改系统时间，以及夏令时结束后调整回标准时间。

时间设置　　将系统的时间设置为您在小时、分钟、秒、年月日字段设置的时间。

与 NTP 服务器同步　　点击“与 NTP 同步校准时间”配置系统使用 NTP 自动设置时间。

服务器 输入 ZXSEC US 设备用来设置系统时间的网络时间协议(NTP）服务器 IP 地址或域名。

同步间隔 指定 ZXSEC US 系统与 NTP 服务器时间校准的间隔。典型的 Syn 间隔为每 1440 分钟，ZXSEC US 设备随 NTP 服务器每天校准系统时间。

3.4 更改 ZXSEC US 设备固件

更改 ZXSEC US 设备主机名称

系统状态的页面上与 CLI 提示符中显示 ZXSEC US 设备主机的名称。主机名称也被

用作 SNMP 系统名称。有关 SNMP 主机名称的详细信息，参见“SNMP 系统名称”。

默认的主机名称时 ZXSEC US 设备的序列号。例如 ZXSEC US1300。

具有对系统配置读取权限的系统管理员可以更改 ZXSEC US 设备主机名称。



注意：

如果 **ZXSEC US** 设备作为 HA 群集的一部分，您应该给设备设置唯一的名称以区别 HA 群集中其它设备的主机名称。

更改 ZXSEC US 设备主机名称

1. 进入系统>状态。
2. 在设备信息区域的主机名称栏，点击“更改”。
3. 在“新名称”字段，输入新的主机名称。
4. 点击 OK 确认。

新的主机名称将在主机名称字段域 CLI 提示符中显示，并添加到 SNMP 系统名称栏中。

更改固件版本

具有对系统配置读取权限的系统管理员可以更改 ZXSEC US 设备固件。

固件更改包括升级到新的固件版本与降级到旧的固件版本。执行以下操作更改固件版本：

升级为新的固件版本

使用以下操作可以将 **ZXSEC US** 设备升级为更新的固件版本。

注意：

安装固件替代您现行的防病毒与攻击定义。安装新的固件后，参见“更新反病毒与更新定义”更新防病毒与攻击定义。

使用基于 web 的管理器升级固件

1. 将固件镜像文件拷贝到您的管理计算机。
2. 使用超级管理员，或对系统具有读写权限的管理员，登录基于 web 的管理器页面。
3. 进入系统管理>状态。
4. 在固件版本选项下，点击“升级”。
5. 输入固件镜像文件的路径与文件名，或点击“浏览”查找文件的位置。
6. 点击 OK 确认。

   ZXSEC US 设备上传固件镜像文件，升级到新的固件版本，重新启动并显示 ZXSEC US 登录页面。该操作过程将花费几分钟的时间。
7. 登录基于 web 的管理器。
8. 进入系统>状态并检查固件版本确认新固件升级成功。
9. 升级防病毒与攻击定义。有关升级防病毒与攻击定义的详细信息，参见 US Service 中心。

恢复为旧的固件版本

执行以下操作可以将固件版本降级为旧的版本。该操作也可以将固件恢复到出厂默认的配置并将删除 IPS 用户定义的特征、web 内容列表、邮件过滤列表以及更改的替换信息。备份 ZXSEC US 设备的配置保存这些信息。

恢复为旧的 USOS 版本（例如，从 USOSv2.80 恢复到 USOSv2.50 版本），从备份的配置文件中，不能恢复旧版本的配置。

注意：

安装固件替代您现行的防病毒与攻击定义。安装新的固件后，参见反病毒与更新定义"确定已经更新了防病毒与攻击定义。

使用基于 web 的管理器恢复为旧的固件版本

1. 拷贝固件镜像到管理计算机。
2. 登录使用管理员帐户，或拥有系统配置读写权限的管理员帐户。登录到 ZXSEC US 基于 web 的管理器。
3. 进入系统>状态。
4. 在系统信息>固件版本项下，点击"升级"。
5. 键入固件镜像文件的路径与文件名，或点击"浏览"查找文件。
6. 点击 OK 确认。

   ZXSEC US 设备上传固件镜像文件，恢复为旧的固件版本，重新设置配置并重新启动，显示 ZXSEC US 登录页面。该操作过程将花费几分钟时间实现。

注意：

安装固件替代您现行的防病毒与攻击定义。安装您的固件后，确保防病毒与攻击定义已经更新。

7. 登录基于 web 的管理器。
8. 进入系统>状态并检查固件版本，确认固件安装成功。
9. 恢复配置。

   有关恢复配置的详细信息，参见 ZXSEC US 管理员指南。
10. 更新防病毒与攻击定义。

3.5 查看设备运行记录

内容

历史记录页面显示 6 个图表，分别表示以下系统资源使用的情况以及病毒与入侵检测的防护状态。

1. 进入“系统>状态”。

2. 点击系统资源栏中右上角的“历史记录”。

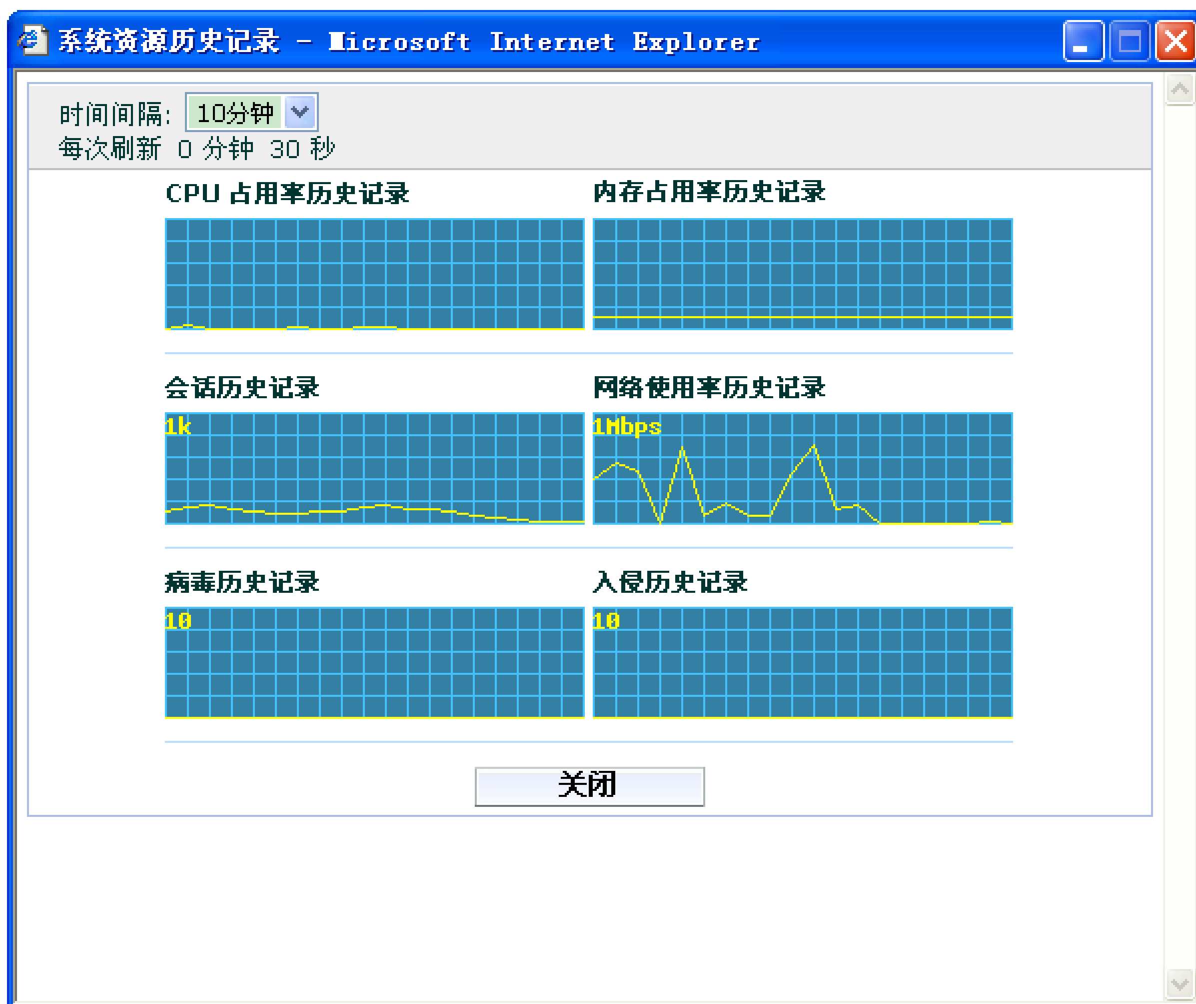


图3.5-1 系统资源使用历史记录举例

间隔 选择显示历史记录的时间间隔。

CPU 占用率历史记录 设定的间隔时间内的 CPU 占用情况。

内存占用率历史记录 设定的间隔时间内的内存使用的历史记录。

会话历史记录设定的间隔时间内的通讯会话的历史记录。

3.6 手工更新 US Service 定义

内容

在系统状态页面中的许可证栏，您可以更新 US Service-AV 与 US Service-入侵。

有关配置 ZXSEC US 设备进行自动 AV 与 IPS 定义更新的详细信息，参见"US Service 中心"。

手工更新 US Service AV 定义

1. 从中兴通讯公司下载最新的 AV 定义，并将其拷贝到您连接基于 web 管理器所使用的计算机。
2. 打开基于 web 的管理器，并进入"系统>状态"。
3. 查看"许可证信息"栏目中的 US Service 订制的 AV 定义字段，点击"更新"。弹出 AV 定义更新对话框。
4. 在"更新文件"字段，输入 AV 定义更新文件的路径与文件名，或点击"浏览"查找 AV 定义更新文件的存放地址。
5. 点击 OK 确认将更新文件上传到 ZXSEC US 设备。ZXSEC US 设备更新 AV 定义文件。需要花费约 1 分钟的时间。
6. 进入"系统>状态"确认 US Service AV 定义版本已经更新。

手工更新 US Service IPS 定义

1. 从中兴通讯公司下载最新的攻击定义更新文件，并将其拷贝到您连接基于 web 管理器所使用的计算机。
2. 打开基于 web 的管理器，并进入"系统>状态"。
3. 查看"许可证信息"栏目中的 US Service 订制的 IPS 定义字段，点击"更新"。弹出 IPS 定义更新对话框。
4. 在"更新文件"字段，输入 IPS 定义更新文件的路径与文件名，或点击"浏览"查找 IPS 定义更新文件的存放地址。
5. 点击 OK 确认将更新文件上传到 ZXSEC US 设备。
6. ZXSEC US 设备更新 IPS 定义文件。需要花费约 1 分钟的时间。
7. 进入"系统>状态"确认 US Service IPS 定义版本已经更新。

3.7 查看统计表

内容

系统状态统计列表提供有关通信会话、内容存档与网络防护活动的信息。

查看通信会话列表

1. 进入“系统>状态”。

2. 统计信息列表中，点击会话对应的“详情”进行查看。

1 / 1 清除所有的过滤条目

#	协议	源地址	源端口	目标地址	目标端口	策略ID	结束(秒)	
1	tcp	10.16.13.53	1133	10.30.1.9	514		23	
2	tcp	10.16.13.53	1131	10.30.1.9	514		3	
3	tcp	10.16.13.53	1139	10.30.1.9	514		113	
4	tcp	10.16.13.53	1137	10.30.1.9	514		83	
5	tcp	10.16.13.53	1135	10.30.1.9	514		53	
6	tcp	10.16.26.180	2562	10.16.13.53	443		20	
7	tcp	10.16.26.180	2560	10.16.13.53	443		36	
8	tcp	10.16.26.180	2574	10.16.13.53	443		83	

图3.7-1 会话列表

虚拟域 点击选择一个虚拟域，列出由该虚拟域处理的通信会话。该选项只有在启动多个虚拟域的情况下可用。更新会话列表。

刷新 更新会话列表

上一页 查看会话列表上一页信息。

下一页 查看会话列表下一页信息。

显示开始行 输入开始显示会话列表的列表行数。例如，如果共有 5 行会话列表，您输入 3，表示显示行数为开始为 3，接着行数为 4，5 的会话。

清除所有过滤器 点击重设会话过滤器设置。

源 IP 设置列表过滤的源 IP 地址。

协议 连接的服务协议。例如 udp，tcp 或 icmp。

间隔 选择显示历史记录的时间间隔。

目的 IP 设置列表过滤的目标 **IP** 地址。

目的端口 设置列表过滤的目标端口。

源端口 设置列表过滤的源端口。

策略 ID 允许会话通过的防火墙策略数量; 如果通讯会话只涉及一个 ZXSEC US 端口（如管理员会话），策略 ID 处显示为空白。删除图标，点击删除动态通信会话。

过期时间 连接过期的时间（以秒计）。

删除图标 停止活动的通信会话。您的访问权限必须是对系统配置能够执行读与写。

应用过滤 确认列表过滤内容。

查看内容存档信息

从系统状态页面中的统计表信息栏，您可以查看通过 ZXSEC US 设备的 HTTP、邮件、FTP 与 IM 流量。您可点击“详情”查看每种流量类型的详细信息。

您可以点击统计信息栏目中“重设”清除内容存档信息与攻击日志信息，并将统计信息归零。

查看存档的 HTTP 内容信息

1. 进入“系统>状态”。
2. 在“内容存档”，点击“详情”查看 HTTP 流量的详细信息。

日期与时间 访问 URL 的时间。

IP 地址 访问的 URL 的 IP 地址。

访问 URL 所访问的 URL。

查看存档的电子邮件内容信息

1. 进入“系统>状态”。
2. 在“内容存档”，点击“详情”查看电子邮件流量的详细信息。

最近会话(会话最大值 96).

日期和时间	来源	目的	主题

长期内容信息存档请访问日志服务设备界面.

关闭

图3.7-2 会话信息

日期与时间 电子邮件通过 ZXSEC US 设备的时间。

发送端 发件人的邮件地址。

目的端 收件人的邮件地址。

主题 邮件的主题。

查看存档的 FTP 内容信息

1. 进入“系统>状态”。
2. 在“内容存档”，点击“详情”查看 FTP 流量的详细信息。

日期与时间 访问的日期与时间。

目的地址 FTP 服务器的 IP 地址。

用户 登录 FTP 服务器的用户 ID。

下载 被下载文件的名称。

上传 上传文件的名称。

查看存档的 IM 内容信息

1. 进入“系统>状态”。
2. 在“内容存档”，点击“详情”查看 IM 流量的详细信息。

日期与时间 访问的日期与时间。

协议 IM 会话使用的协议。

种类 IM 流量的种类。

本地地址 该流量处理的本地地址。

远程地址 该流量处理的远程地址。

方向 文件是被发送货被接收。

查看攻击日志

从系统状态页面中的统计表信息栏，您可以查看 ZXSEC US 设备阻止的网络攻击。您可点击“详情”查看每项攻击的详细信息。

您可以点击统计信息栏目中“重设”清除内容存档信息与攻击日志信息，并将统计信息归零。

查看拦截的病毒信息

1. 进入“系统>状态”。
2. 在“攻击日志”中，点击“详情”查看 AV 信息。

日期与时间 检测到病毒的日期与时间。

来自 发件人的邮件地址或 IP 地址。

到达 目的接收人的邮件地址或 IP 地址。

服务 服务类型，如 POP 或 HTTP。

病毒 被检测到的病毒名称。

查看被屏蔽的攻击

1. 进入“系统>状态”。
2. 在“攻击日志”中，点击“详情”查看 IPS 信息。

日期与时间 检测到攻击的日期与时间。

来自 攻击的来源。

目标 攻击针对的目标主机。

服务 服务类型。

攻击 被检测与阻止的攻击类型。

查看垃圾邮件信息

1. 进入“系统>状态”。
2. 在“攻击日志”中，点击“详情”查看垃圾邮件信息。

日期与时间 检测到垃圾邮件的日期与时间。

收发件人 IP 地址 发件人与收件人的 IP 地址。

收发件人邮件地址 发件人与收件人的邮件地址。

服务 服务类型，如 SMTP、POP 或 IMAP。

垃圾邮件类型 所检测到的垃圾邮件的类型。

查看屏蔽的 URL

1. 进入“系统>状态”。
2. 在“攻击日志”中，点击“详情”查看屏蔽 URL 的信息。

日期与时间 检测到试图访问的 URL 的时间。

来自 试图查看 URL 的主机。

屏蔽的 URL 被屏蔽的 URL。

第4章 系统虚拟域

4.1 概述

描述

本章将对如何在 ZXSEC US 设备中配置并使用虚拟域，使 ZXSEC US 设备能够作为多个虚拟设备进行操作，对多个网络提供单独的防火墙与路由策略。

内容

本章内容如下：

4.2 虚拟域

内容

虚拟域的设置可以使一台 ZXSEC US 设备能够根据服务商的管理安全服务对多重网络提供独立的防火墙与路由服务。

VDOM 提供独立的安全域，允许配置并管理单独的区域、用户验证、防火墙策略、路由与 VPN 配置。VDOM 的设置简化了配置，您不需要单独管理许多的路由与防火墙策略。

启动虚拟域配置后，配置并使用 VDOM。

创建并配置 VDOM 时，必须对 VDOM 分配接口或 VLAN 子接口。或者，可以对配置的 VDOM 分配一个管理帐户，通过管理帐户登录 VDOM。如果 VDOM 是创建服务于一个机构，那么该机构可以单独的对该 VDOM 进行管理。对于每个 VDOM，可以应用不同的操作模式，NAT/路由或透明模式。

当一个数据包进入 ZXSEC US 设备中的一个虚拟域时，它将被限制在这个虚拟域中。在一个给定的域中，您只能够对 VLAN 子接口与区域之间的连接创建防火墙策略。数据包不能够跨越域的边界。数据包在 VDOM 之间穿越必须通过物理接口上设置的防火墙策略。然后数据包到达其他 VDOM 的不同接口，在进入该接口之

前必须通过接口设置的防火墙策略。数据包穿越的VDOM是创建在同一个ZXSEC US 设备中。唯一的例外是使用 CLI 命令可以配置 VDOM 间的路由。

ZXSEC US 设备的其他功能是可以进行全局配置的。这样的功能配置可以应用于所有的 VDOM。也就是说可以统一配置入侵防护、反病毒与 web 过滤配置等。同样，VDOM 之间可以共享固件版本、反病毒与攻击数据库。

默认的情况下，ZXSEC US 设备最大支持应用于 NAT/路由或透明模式的 10 个 VDOM。

**注意：**

ZXSEC US350A 设备的交换模式不支持 VDOM。

虚拟域配置启动后，您可以使用默认的 admin 帐户登录，进入“系统>状态”页面，在许可证信息栏目查看 ZXSEC US 设备所支持的最大虚拟域应用数量。

默认情况下，每台 ZXSEC US 都设置了名为 root 的一个虚拟域。该虚拟域包括全部的 ZXSEC US 物理接口，VLAN 子接口，区域，防火墙策略，路由设置与 VPN 设置。

SNMP、日志、警报邮件、基于 US SERVICE 中心的更新与基于 NTP 的时间设置这样的管理系统是使用管理 VDOM 中的地址与路由与外部网络通信。只能连接到与管理虚拟域通信的网络资源。默认的管理虚拟域是根虚拟域，不能进行修改。

当您添加一个虚拟域时，您可以配置添加 VLAN 子接口，区域，防火墙策略，路由设置以及 VPN 设置。您也可以将 root 虚拟域的物理接口转移到其它虚拟域，或是将 VLAN 子接口从一个虚拟域中转移到另一个虚拟域中。

有关 VDOM 的详细信息，参见 ZXSEC US 设备 VLAN 与 VDOM 使用手册。

VDOM 配置设置

以下的配置设置必须是每个 VDOM 单独配置的，不能在 VDOM 之间共享。VDOM 的常规管理员只能查看其设置，默认的超级管理员能够访问这些设置，但是这之前，需要选择所要查看的 VDOM。

- 系统设置

  区域

DHCP 服务

操作模式（NAT/路由或透明）

管理 IP（透明模式）

- 物理接口

VLAN 子接口

区域

管理 IP（透明模式）

- 路由配置
- 防火墙设置

策略

地址

服务组与用户定义服务

排程

IP 池

内容保护列表

- VPN 配置

IPSec

PPTP

SSL

- 用户设置

用户

用户组

RADIUS 与 LDAP 服务器

微软 Windows 活动目录服务器

- P2P 统计表（查看/重设）
- 日志配置，日志访问或日志报告

全局配置设置

所有的虚拟域共享以下配置设置。即使您配置了多重虚拟域，配置以下设置的方法是不变的：

- 设备配置

  物理接口与 VLAN 子接口（每个物理或 VLAN 子接口只能属于一个VDOM。每个 VDOM 也只能够配置属于自己的接口。）

  DNS 设置

  主机名称，系统时间，固件版本（在“系统状态”页面配置）

  闲置与验证超时

  基于 web 的管理器的现实语言

  LCD 面板 PIN，适用范围

  失效网关检测

  HA 配置

  SNMP 配置

  替换信息设置

  管理员设置（每个管理员只能属于一个 VDOM。各个 VDOM 也只能够被所属管理员进行配置。）

  访问控制列表

  USM 配置

  配置备份与恢复

  US SERVICE 中心更新配置

  BUG 报告

- VPN 证书
- 反病毒配置
- 入侵防护配置
- web 过滤配置
- 反垃圾邮件配置

- IM 配置
- 统计表设置
- 用户列表与策略

4.3 启动虚拟域

内容

使用默认的 admin 管理帐户，您可以配置 ZXSEC US 设备启动多个 VDOM 操作。

启动虚拟域

1. 使用 admin 帐户登录登录基于 web 的管理器。
2. 进入“系统>状态”页面。
3. 在系统信息栏中“虚拟域”设置，点击“启动”。

您登录的帐户自动退出。您可以使用 admin 再登录。

虚拟域启动后，基于 web 的管理器与 CLI 发生如下变化：

- 全局配置与每个 VDOM 的配置相互独立。
- 系统页面下出现新的 VDOM 条目。
- 只有使用 admin 帐户能够查看或配置全局配置。
- Admin 帐户可以配置所有 VDOM 的配置。
- Admin 既可以从根 VDOM 下的任何接口连接也可以通过任何分配了常规管理员的 VDOM 访问。
- 常规管理员只能配置属于各自的 VDOM,也只能够从所属的 VDOM 的接口登录访问 ZXSEC US 设备。

启动虚拟域后，您可以从屏幕左下方查看当前的虚拟域信息，显示格式为“当前虚拟域：虚拟域名称”。

配置虚拟域与全局设置

虚拟域启动后，只有默认的超级管理员帐户能够进行以下配置：

- 配置全局设置
- 创建或删除 VDOM

- 配置多个 VDOM
- 对 VDOM 分配接口
- 对 VDOM 分配管理员

一个 VDOM 只有在包含至少两个物理接口或虚拟子接口分别用于向内与向外的流量时才是有用的。只有超级 admin 可以对 VDOM 分配接口或子接口。常规管理员可以在属于各个的 VDOM 的物理接口中创建一个 VLAN 子接口。

在没有对 VDOM 创建并分配常规管理员之前，只有超级管理员可以配置 VDOM。

只有超级管理员可以对 VDOM 分配管理员。对“管理员用户”具有读与写的访问权限时可以在所属的 VDOM 中创建额外的管理员。

4.4 配置 VDOM 与全局配置

内容

启动 **VDOM** 与配置全局设置

在启动虚拟域的情况下以 admin 登录时，您将自动登录到全局配置，系统页面下将显示 VDOM 选项。

进入“系统>VDOM”，配置虚拟域。

新建　　管理虚拟域: root　　应用

启用	名称	操作模式	接口	注释	
☑	root	NAT	loop1 , port1 , port10 , port2 , port3 , port4 , port5 , port6 , port7 , port8 , port9 , ssl.root		

图4.4-1　VDOM 列表

新建　　添加新的虚拟域。输入新的 VDOM 名称并点击 OK 确认。VDOM 的名称设置不能与现有的 VDOM，VLAN 或区域重名。VDOM 的名称最大可以设置不包含空格的 11 个字符。

管理　　用于系统管理的虚拟域。管理虚拟域是加括号标示的。默认的管理 VDOM 是根虚拟域。如果在设置管理虚拟域时选择了不止一个虚拟域，第一个出现在列表中的 VDOM 将被分配作为管理虚拟域。

删除　　删除所选的 VDOM。根虚拟域不能被删除。

切换 点击进入所选虚拟域。您可以从屏幕左下方查看当前的虚拟域信息，显示格式为“当前虚拟域：虚拟域名称”。全局设置显示的屏幕下在该位置则没有 VDOM 名称显示。

名称 VDOM 的名称。

操作模式 VDOM 的操作模式，NAT 或透明模式。

接口 与 VDOM 连接的接口，包括虚拟接口。

管理虚拟域 显示管理虚拟域。所有非管理虚拟域在本栏中均会显示为“非（NO）”。

在虚拟域中添加 VDOM

一个虚拟域必须包含至少两个接口，可以是物理接口也可以是 VLAN 接口。默认情况下，所有的物理接口都属于根虚拟域。

在 USOS v3.0 MR1 中。VDOM 间的路由功能可以在不使用物理接口的情况下在 VDOM 之间进行内部通信。VDOM 间通信的功能只能通过 CLI 配置，详细信息参见 ZXSEC US 设备 CLI 使用参考手册与 ZXSEC US 设备 VLAN 与 VDOM 配置手册。

相比较物理接口，VLAN 子接口常常需要被分配到不同的 VDOM。这种情况下，超级管理员必须先创建 VDOM，然后创建 VLAN 子接口并将其分配到所需的 VDOM。

只有在全局设置下，进入“系统>网络>接口”项下进行接口配置，该操作在任何 VDOM 都不可用。有关创建 VLAN 子接口的详细信息，参见“添加 VLAN 子接口”。

分配接口到 VDOM

以下操作是有关如何将现有的接口重新从一个虚拟域中分配到其他虚拟域中。

假设前提是启动了虚拟域且设置了不止一个虚拟域。

如果虚拟域应用了任何配置，则不可以被删除；例如 VDOM 中含有接口。如果在 VDOM 中的接口应用了以下配置，则不能被删除：

- DHCP 服务器
- 区域
- 路由
- 防火墙策略

- IP 池
- 代理 arp（只能使用 CLI 访问）

在删除接口之前，需要删除或修改接口的衣裳配置。

**注意：**

接口或子接口中删除图标显示可用时，接口或子接口可以被重新分配或删除。没有显示可删除图标，表示接口在应用其他配置。

分配接口到虚拟域

1. 使用 admin 帐户登录。
2. 进入系统>网络>接口。
3. 选择准备分配的接口，点击“编辑”接口。
4. 选择接口所要移动到的目标虚拟域。
5. 根据需要配置其他配置并点击 OK 确认。

接口转移到虚拟域中。对接口设置的防火墙 IP 池域虚拟 IP 将被删除。您应该手动删除接口包含的任何路由，并对接口创建新的路由。否则您的流量将不能够正常的进行路由。

分配管理员到 VDOM

如果您对一个机构或公司创建了虚拟域，用于管理该机构的网络资源，您需要同时创建属于该 VDON 的虚拟域。

创建属于一个 VDOM 的管理员可以更改所属虚拟域的配置，但不能配置能够影响 ZXSEC US 设备中其他 VDOM 的设置。

分配到 VDOM 的常规管理员只能使用属于该 VDOM 接口登录基于 web 管理器或 CLI。超级管理员可以从 ZXSEC US 设备中任何允许管理访问的接口连接到基于 web 的管理器或 CLI。只有超级管理员或根虚拟域的常规管理员 ton 通过连接控制接口登录。

分配管理员到 VDOM

1. 使用超级管理员帐户登录。虚拟域必须已启动。
2. 进入“系统>Admin>管理员”。

3. 创建和/或配置新的管理员帐户。有关配置管理员帐户的其他信息，参见“配置管理员帐户”。

4. 配置该管理员帐户时，从虚拟域列表中选择该管理员所属的虚拟域。

5. 点击“应用”确定。

更改管理 VDOM

US 设备的管理虚拟域是一些默认的流量类型发出的窗口,所述这些类型的流量包括：

- SNMP
- 日志流量
- 警报邮件
- 基于 US SERVICE 中心更新
- 基于 NTP 的时间设置

在更改管理 VDOM 之前，确定虚拟域已经启动。

ZXSEC US 设备中只能设置存在一个管理 VDOM如果您在设置管理 VDOM 时选择了不止一个 VDOM，那么位于列表顶端的 VDOM 将成为管理 VDOM。

注意：

任何管理员正在使用 RADIUS 验证期间，不能更改管理 VDOM。

更改管理 VDOM

1. 进入“系统>VDOM”。

2. 选择作为管理 VDOM 的虚拟域。

3. 点击“管理”应用设置更改。

管理流量将通过新的管理 VDOM 发出。

第5章 网络配置

5.1 概述

描述

设置系统网络是指怎样将 US 设备配置到网络中作为防火墙设备生效。基本的网络设置包括配置 ZXSEC US 设备的接口与您的网络连接，以及配置 ZXSEC US 的 DNS 设置。更多高级的配置包括在设备网络配置中添加 VLAN 子接口与区域。

- 接口
- 区域
- 网络选项
- 路由表（透明模式）
- 配置调制解调器接口
- VLAN 概述
- NAT/路由模式下配置 VLAN
- 透明模式下配置 VLAN
- US Ipv6 支持

注意：

在相同字段，您可以输入 IP 地址与掩码，掩码可以使用简短形式。例如，192.168.1.100/255.255.255.0 也可以输入为 192.168.1.100/24。

接口

NAT/路由模式下，进入“系统>网络配置>接口”，配置 ZXSEC US 接口。您可以：

- 修改物理接口的配置。
- 添加并配置 VLAN 子接口。
- 配置 ADSL 接口。
- 将几个物理接口聚合成为一个 IEEE802.3AD 接口只适用于 ZXSEC US1300

以及更高型号设备）。

- 配置物理接口作为冗余接口。
- 查看回环与 VDOM 间的链接接口。

注意：

本章节中，除非另有注明，所述接口指 ZXSEC US 设备的物理接口或 VLAN 子接口。

有关透明模式下配置 VLAN 的详细信息，参见“ZXSEC US 设备与配置 VLAN”。

新建 [栏式设置]

名称	IP/掩码	访问控制	管理状态	
port1	192.168.1.99 / 255.255.255.0	HTTPS,PING		
port10	0.0.0.0 / 0.0.0.0	PING		
port2	10.16.13.53 / 255.255.255.0	HTTPS,PING,SSH,TELNET,SNMP		
port3	0.0.0.0 / 0.0.0.0	PING		
port4	0.0.0.0 / 0.0.0.0	PING		
port5	0.0.0.0 / 0.0.0.0	PING		
port6	0.0.0.0 / 0.0.0.0	PING		
port7	0.0.0.0 / 0.0.0.0	PING		
port8	0.0.0.0 / 0.0.0.0	PING		
port9	0.0.0.0 / 0.0.0.0	PING		

图5.1-1 接口列表（常规管理员所查看）

新建 [栏式设置]

名称	IP/掩码	访问控制	管理状态	
port1	192.168.1.99 / 255.255.255.0	HTTPS,PING		
port10	0.0.0.0 / 0.0.0.0	PING		
port2	10.16.13.53 / 255.255.255.0	HTTPS,PING,SSH,TELNET,SNMP		
port3	0.0.0.0 / 0.0.0.0	PING		
port4	0.0.0.0 / 0.0.0.0	PING		
port5	0.0.0.0 / 0.0.0.0	PING		
port6	0.0.0.0 / 0.0.0.0	PING		
port7	0.0.0.0 / 0.0.0.0	PING		
port8	0.0.0.0 / 0.0.0.0	PING		
port9	0.0.0.0 / 0.0.0.0	PING		

图5.1-2 启动虚拟域后的接口列表显示（超级管理员查看）

新建 点击“新建”创建一个 VLAN。型号为 800 或更高的设备，您还能够创建一个 IEEE802.AD 聚合接口。

交换模式点击在交换模式与接口模式之间切换。交换模式下所有的内部接口都集中在一个接口中。接口模式下，每个接口都配置了所属的接口。切换模式之前，所有对"内部接口"的配置都需要删除。该选项只适用于 Rev2.0 或更高的 US180 与 US350 设备。

显示背板接口　　点击使两个背板接口成为可见接口 port9 与 port10。接口可见后可以如同常规物理接口一样操作。该选项只适用于 US9000 系列的设备。

描述图标　　点击该图标显示接口的"描述"字段。

名称　　ZXSEC US 设备中物理接口名称显示，包括接口所配置的别名。

物理接口的名称与数量是由 ZXSEC US 设备的型号决定的。一些接口的名称指示了接口默认的功能（例如，内部接口、外部接口与 DMZ）其他接口的名称是通用的，如 port1。

ZXSEC US1300 或更高型号的设备中，如果您配置将几个接口作为聚合接口，接口列表中只显示聚合接口，并不一一显示组成聚合接口的各个接口。这样的规则同样适用于冗余接口。参见"创建 802.3AD 聚合接口"与"创建冗余接口"。

对于应用于交换模式下的 ZXSEC US350A，port1 到 port26 是不显示的。这些都是交换-VLAN 接口。参见"查看交换-VLAN 端口"。

如果您添加了 VLAN 子接口，这些子接口也会在名称列表中被添加的 ZXSEC US 设备物理接口后中列出。参见"VLAN 概述"。

如果配置了回环或 VDOM 间的接口，您可以在列表中查看到所配置的接口。这样类型的接口只有使用 CLI 进行编辑。有关这些接口的详细信息，参见"需使用 CLI 才可配置的接口"章节，或参见 ZXSEC US 设备 CLI 使用参考手册中对命令 config system interface 与 config system inter-vdom 的叙述。

如果启动了虚拟域配置，在不适用超级管理员帐户登录的情况下，您只可以查看当前虚拟域中的接口。

如果对 Rev.2.0 或更高版本的 ZXSEC US180 或 US350 或 ZXSEC US120 与 ZXSEC US120W 设备启动了接口模式，您将查看到多个内部接口。

如果切换到交换模式，便只有一个内部接口。

如果您使用的 ZXSEC US 设备支持 AMC 模块以及您已经安装了 AMC 模块，那么该模式中的接口，如 USASM-FB4 具有 4 个接口，将被添加在接口列表中并显示。这些 AMC 的接口依次命名为 AMC/1，AMC/2 等。

IP/掩码地址 当前接口的 IP/掩码地址。

虚拟域 点击虚拟域显示添加到该虚拟域上的所有接口。只有在您添加了虚拟域后，该操作才有效。

访问权限 接口的管理访问配置。有关管理访问选项的信息，参见“控制到接口的管理访问”。

状态 接口的管理状态。如果管理状态呈绿色箭头表示接口已经激活能够接收网络通讯。如果管理状态呈红色箭头表示接口不能接收网络通讯数据。点击“发起”或“关闭”可以更改管理状态。删除，编辑与查看图标。

交换模式

ZXSEC US180，US350 设备中的内部接口是四个接口的交换。通常情况下，内部接口配置作为一个能够被四个接口共享的接口。应用于交换模式，您可以配置交换机上配置每个接口与交换机本身的接口相互独立。ZXSEC US120 与 ZXSEC US120W 的内部接口是 6 端口的交换机模式，功能相同。

交换模式功能体现在两个方面：交换模式与接口模式。交换模式是默认的模式，只有一个接口应用于整个内部信息交换。接口模式下，可以单独配置每个内部交换接口。那么，便可以对每个内部接口分配不同的子网与掩码。

交换模式只能应用在 Rev.2.0 与更高级别的 ZXSEC US180 与 US350 设备。有关交换模式功能被支持的最新的设备型号列表，参见 ZXSEC US 设备发布说明。

打开“系统>网络>接口”，可以进入“交换模式管理”页面，配置交换模式。

**警告：**

在进行交换模式与接口模式之间相互切换的操作之前，接口所配置的设置必须删除。这样的设置包括防火墙策略路由DNS转发DHCP服务VDOM接口分配、VLAN应用。如果不删除这些设置便不能执行模式的切换，强制执行后将弹出错误信息提示。

交换模式 点击切换到交换模式。该模式下只显示一个内部接口。

接口模式 点击切换到接口模式。交换机的所有内部接口均显示作为可单独配置的接口。

确认 点击保存设置更改并返回接口界面。

取消 点击取消设置更改并返回接口界面。

使用 CLI 配置交换模式

除了 GUI 界面中配置管理交换模式，还可以使用 CLI 命令对该功能进行配置：

```
config system global
set internal-switch-mode {interface | switch}
end
```

如同在 GUI 配置，模式切换之前需要先删除接口的配置，否则操作中将弹出错误信息提示。在您删除接口的设置后，ZXSEC US 设备将重新启动并进入新的交换模式。

详细信息，参见 ZXSEC US 设备 CLI 使用参考手册中有关命令 config system global 的叙述。

接口设置

进入“系统>网络>接口”点击“新建”创建新的接口。 对现有接口进行编辑时，

点击接口对应的编辑图标。一些类型的接口，例如回环与 VDOM 间的接口只能够使用 CLI 命令进行配置。

该页面下，您不能创建虚拟 IPSec 接口，但是您可以指定 IPSec 接口的终端地址，启动接口的管理访问并对接口进行描述。更多信息，参见“配置虚拟 IPSec 接口”。

配置交换模式下的 ZXSEC US350A 设备的交换接口，参见“配置交换-VLAN 接口”。

新建接口	
接口名称	
类型	VLAN
接口	port1
VLAN ID	
虚拟域	root

图5.1-3 创建新的接口设置

地址模式
自定义 DHCP PPPoE
IP地址/网络掩码: 0.0.0.0/0.0.0.0
DDNS 启用
Ping服务器 启用
管理访问 HTTPS PING HTTP
SSH SNMP TELNET
二级IP地址
描述（63 多个字符）
确定 取消 应用

图5.1-4 编辑接口设置

名称 接口的名称。现有接口的名称不能更改。

别名 输入对接口设置的其他名称。设置别名是为了容易识别不同的接口。别名设置只能应用于还没有配置名称的物理接口。别名的最大设置长度为 15 个字符。别名不是接口名称的一部分，但是会在接口名称旁边，加括弧显示。日志中不显示别名。

类型 在 ZXSEC US1300 或该型号以上的设备，您可以创建 VLAN，802.3AD 聚合接口以及冗余接口。

- 其他型号的设备只支持创建 VLAN 接口，且没有类型字段设置。
- 配置 VLAN 接口的详细信息参见“配置 VLAN 接口”章节的叙述。
- 配置聚合接口的详细信息，参见“配置聚合接口”章节的叙述。
- 配置冗余接口的详细信息，参见“配置冗余接口”章节的叙述。
- 配置无线接口的详细信息，参见“配置无线接口”章节的叙述。

现有接口的类型不能更改。

接口 点击接口的名称添加到接口的 VLAN 子接口。所有的 VLAN 子接口必须与物理接口建立连接。连接建立后，在接口的列表中显示的物理接口后边列出

VLAN 子接口名称。现有接口的 VLAN 子接口不能更改，将类型设置为 VLAN 时，不显示该字段。

物理接口成员将接口从可用接口列表中移动到被选接口列表，用于创建802.3AD聚合接口或冗余接口。当接口类型设置为802.3AD聚合或冗余接口时，不显示该字段。

VLAN ID　输入的VLAN ID需要与该VLAN子接口接收数据包的VLAN ID相匹配。您不能够更改现有的VLAN子接口的VLAN ID。

寻址模式选择“手工”配置接口使用静态 IP 地址。您也可以对接口配置使用动态 IP 地址。

虚拟域　选择虚拟域添加到该虚拟域的接口或 VLAN 子接口如果您添加了虚拟域，该操作才能够生效。

IP/掩码 输入IP地址与子网掩码。设置的IP地址与接口连接的网络必须在相同的子网。两个接口不能设置在相同子网的IP地址。该字段只有在寻址模式设置为手工时可用。点击该选项对接口配置动态DDNS服务。

DDNSPing 服务器　选择虚拟域添加到该虚拟域的接口或 VLAN 子接口如果您添加了虚拟域，该操作才能够生效。

管理访问设置接口管理访问类型。

HTTPS PING　通过该接口允许到基于 web 管理器安全的 HTTPS 连接。如需要该接口对 ping 命令作出响应。使用该设置校正安装并可用于检测。

HTTP　通过该接口允许到基于web管理器安全的HTTP连接。HTTP并不安全并且可以被第三方截取。

SSH　通过该接口允许要 CLI 的 SSH 连接。

SNMP　通过连接到该接口允许远程 SNMP 管理器请求 SNMP 信息。

TELNET通过该接口允许到 CLI 的 Telnet 连接。Telnetl 连接并不安全并且容易被第三方截取。更改 MTU，点击“代理默认 MTU 值（1500）”并根据接口的寻址模式输入 MTU 容量。

MTU

静态模式设置为 68 到 1500 字节。

手动与 DHCP 寻址模式设置为 576 到 1500 字节。

PPPoE 寻址模式 MTU 容量可以设置为 576 到 1492 字节。

对于巨帧（US6010 以及该型号以上的设备），最大可以设置为 16110 字节。

该字段只有在物理接口下可用。VLAN 将默认继承其所属接口的 MTU 容量。

二级 IP 地址 点击接口对应的蓝色箭头扩展或隐藏接口的其他 IP 地址选项。

描述 可选项，输入最多 63 个字符的描述信息。

**注意：**

透明模式下，如果更改一个接口的 MTU，必须更改所有接口的 MTU 与新的 MUT 相匹配。

创建 802.3AD 聚合接口

您可以将两个或多个物理接口聚合（结合）增加带宽并提供一些链接冗余。设置聚合接口的优点在于增加了带宽，但是相比较冗余接口存在更多的潜在故障点。所聚合的接口必须连接在相同的下一跳路由目标。

ZXSEC US1300 以及更高型号的设备固件对于链接聚合执行 IEEE 802.3AD 标准。

接口只有在以下情况下可以用于聚合接口：

- 物理接口，且不是 VLAN 接口。
- 没有作为聚合或冗余接口的一部分。
- 在相同的 VDOM 作为被聚合的接口。
- 没有配置 IP 地址，且没有设置应用 DHCP 或 PPPoE 的接口。
- 没有应用 DHCP 服务器或中继的接口。
- 没有设置任何 VLAN 的接口。
- 没有配置应用任何防火墙策略、VIP、IP 池或多播策略的接口。
- 非 HA 心跳接口。
- 非 US9000 系列设备中的背板接口。

注意：

在您将加速接口（FA2 接口）添加到聚合链接时，便抵消了接口的加速功能。例如，聚合两个加速接口将导致比两个接口单独使用时更慢的吞吐量。

如何接口被征用于聚合接口，该接口将不在“系统>网络>接口”页面的列表中显示。用于聚合接口中的接口将不能再配置防火墙策略、VIP、IP 池或路由。

新建接口

接口名称
类型 802.3ad会聚
虚拟域 root

物理接口成员：
可用的接口 被选的接口
port10
port3
port4
port5
port6

地址模式
自定义 DHCP PPPoE
IP地址/网络掩码： 0.0.0.0/0.0.0.0

DDNS 启用
Ping服务器 启用
管理访问 HTTPS PING HTTP
SSH SNMP TELNET
MTU 分解大于MTU的输出包， 1500 (字节)

图5.1-5 802.3AD 聚合接口设置

创建 802.3AD 聚合接口

1. 进入“系统>网络>接口”。
2. 点击“新建”。
3. 输入聚合接口的名称。接口的名称不能与任何其他接口、区域或 VDOM 重名。

4. 从“类型”列表中，选择 802.3AD 聚合。
5. 同时，从可用接口列表中选择配置组成聚合接口的接口，点击方向箭头移动到所选接口列表中。
6. 如果该接口应用于 NAT/路由模式，您需要对接口配置寻址模式。有关动态寻址的详细信息，参见“配置接口应用 DHCP”与“配置接口应用 PPPoE 与 PPPoA”。
7. 根据需要配置其他选项。
8. 点击 OK 确认。

5.2 配置冗余接口

内容

您可以将两个或多个物理接口结合提供链接冗余。该功能允许您连接到两个或更多的交换机，在发生物理接口或与接口连接的设备故障时保证连接性。

冗余链接不同于聚合链接，任何时间内流量只经过一个接口（无论冗余链接中有多少流量），但是冗余接口允许更巩固的配置减少故障点。这对于全网状 HA 配置很重要。

ZXSEC US1300 以及更高型号的设备可以应用冗余接口。

接口可以配置作为冗余接口的条件是：

- 物理接口，且不是 VLAN 接口。
- 没有作为聚合或冗余接口的一部分。
- 在相同的 VDOM 作为被聚合的接口。
- 没有配置 IP 地址，且没有设置应用 DHCP 或 PPPoE 的接口。
- 没有应用 DHCP 服务器或中继的接口。
- 没有设置任何 VLAN 的接口。
- 没有配置应用任何防火墙策略、VIP、IP 池或多播策略的接口。
- 没有被 HA 监控的接口。

如何接口被征用于冗余接口，该接口将不在“系统>网络>接口”页面的列表中显示。用于冗余接口中的接口将不能再配置防火墙策略、VIP、IP 池或路由。

新建接口

接口名称

类型 冗余接口

虚拟域 root

物理接口成员:

可用的接口 port10 port3 port5 port6 port7

被选的接口 port4

地址模式

自定义 DHCP PPPoE

IP地址/网络掩码: 0.0.0.0/0.0.0.0

DDNS 启用

Ping服务器 启用

管理访问 HTTPS PING HTTP SSH SNMP TELNET

MTU 分解大于MTU的输出包, 1500 (字节)

图5.2-1 冗余接口设置

1. 进入“系统>网络>接口”。
2. 点击“新建”。
3. 输入冗余接口的名称。接口的名称不能与任何其他接口、区域或 VDOM 重名。
4. 从“类型”列表中，选择冗余接口。
5. 同时，从可用接口列表中选择配置组成冗余接口的接口，点击方向箭头移动到所选接口列表中。您从可用接口列表选择接口的顺序将在所选接口列表中体现。例如，如果接口列表中第一个接口故障，第二个接口将接续被使用。
6. 如果该接口应用于 NAT/路由模式，您需要对接口配置寻址模式。有关动态寻址的详细信息，参见“配置接口应用 DHCP”与“配置接口应用 PPPoE 与 PPPoA”。

7. 根据需要配置其他选项。

8. 点击 OK 确认。

5.2.1 配置接口应用 DHCP

内容

配置 ZXSEC US 接口使用 DHCP 后，接口将自动能够播放 DHCP 请求。接口的 IP 地址是 DNS 服务器随机分配的，默认的网关地址同样也是 DHCP 服务器所提供。

进入系统管理>网络>接口。点击“新建”或现有接口对应的编辑图标。在“寻址模式”栏选择 DHCP。

新建接口

接口名称

类型 VLAN

接口 port1

VLAN ID

虚拟域 root

地址模式

自定义 DHCP PPPoE

管理距离： 1

从服务器中重新得到网关。

改变内部DNS。

图5.2-2 接口 DHCP 设置

状态 显示 ZXSEC US 设备与 DHCP 连接的 DHCP 状态信息以及寻址信息。点击“状态”刷新寻址模式状态信息。

初始连接 没有网络活动。

正在连接 接口试图与 DHCP 服务器建立连接。

完成连接 接口从 DHCP 服务器获取了 IP 地址，掩码以及其它设置。

连接失败 接口不能从 DHCP 服务器获取了 IP 地址以及其它信息。

获取 IP/掩码 从 DHCP 服务器租用的 IP 地址与掩码只有在状态显示“完成连接”时，该字段才显示。

更新 点击更新接口的 DHCP 许可证。只有在状态显示“完成连接”时，该字段才显示。

过期 租用的 IP 地址与掩码过期的时间，不是有效的地址。

默认网关 DHCP 服务器分发的网关 IP 地址。只有在状态显示“完成连接”时，该字段才显示，且“从服务器接收默认网关”的功能框是被选的。

管理距离 输入默认从 DHCP 服务器获取默认网关的管理距离参数。管理距离可以设置未 1 到 255 之间的整数指定在多个路由到相同目的地的情况下选择一条当对较为优先的路由管理距离越小表示其路由资源越值得信赖。默认网关的管理距离设置为 1。

从服务器获取默认网关 启动“获取默认网关”从 DHCP 服务器获取默认的网关的 IP 地址。默认的网关将被添加到静态路由表中。

代理内部 启动“代理内部服务器”（Override internal DNS）使用从 DHCP 获取。

DNS DNS 地址代替 DNS 页面中 DNS 服务器的 IP 地址。

连接到服务器 启动“连接到服务器”（Override internal DNS）那么接口将自动试图与 DHCP 服务器建立连接。如果您配置接口未与网络连接将不能启动该选项。

5.3 配置接口应用 PPPoE

内容

如果配置接口使用 PPPoE，ZXSEC US 设备将自动发送一个 PPPoE 请求。如果你配置 ZXSEC US 设备未与网络连接以及您不愿意使 ZXSEC US 设备发送 PPPoE 请求，您可以断开到服务器的连接。

ZXSEC US 设备支持许多 PPPoE RFC 功能（RFC2516）包括未编号 IP，PPPoE 有效发现终止（PADT）。

进入系统管理>网络>接口。点击“新建”或现有接口对应的编辑图标。在“寻址模式”栏选择 PPPoE。

新建接口

接口名称	
类型	VLAN
接口	port1
VLAN ID	
虚拟域	root

地址模式

○ 自定义 ○ DHCP ◉ PPPoE

用户:	
密码:	
无编号IP:	0.0.0.0
初始化Disc超时:	0
初始化PADT超时:	0
管理距离:	1

☑ 从服务器中重新得到网关.

☑ 改变内部DNS.

图5.3-1 接口 PPPoE 设置

状态 显示 ZXSEC US 设备与 PPPoE 连接的 PPPoE 状态信息以及寻址信息。点击"状态"刷新寻址模式状态信息。该字段只有在您选择"编辑"功能框后显示。

初始连接 没有网络活动。

正在连接 接口试图与 PPPoE 服务器建立连接。

完成连接 接口从 PPPoE 服务器获取了 IP 地址，掩码以及其它信息。

连接失败 接口不能从 PPPoE 服务器获取了 IP 地址以及其它信息。

重新连接 重新连接到 PPPoE 服务器。只有在状态是"完成连接"时，该信息字段才显示。

用户名 PPPoE 帐户用户名。

密码 PPPoE 帐户密码。

未编号 IP 指定接口的 IP 地址。如果您的 ISP 服务商分配给您一批 IP 地址，使用其中的一个。否则，该 IP 地址可能与其它接口的 IP 地址相同或作为任何其它 IP 地址。

初始发现超时 重新开始一个 PPPoE 有效发现之前的等待时间。设置初始发现的时间为 0 将在任何时间下都不会终止会话。

初始 PADT 超时时间 如果闲置的时间超出了设置的时间，PPPoE 将被关闭。PADT 功能需要 ISP 服务商的支持。设置初始 PADT 的时间为 0 将在任何时间下都不会终止会话。

管理距离 输入默认从 PPPoE 服务器获取默认网关的管理距离参数。管理距离可以设置未 1 到 255 之间的整数,指定在多个路由到相同目的地的情况下选择一条当对较为优先的路由管理距离越小表示其路由资源越值得信赖默认网关的管理距离设置为 1。

从服务器获取默认网关 启动"获取默认网关"从 PPPoE 服务器获取默认的网关的 IP 地址。默认的网关将被添加到静态路由表中。

代理内部 DNS 启动"代理内部服务器"（Override internal DNS）使用从 PPPoE 获取的 DNS 地址代替 DNS 页面中 DNS 服务器的 IP 地址。

连接到服务器 启动"连接到服务器"(Override internal DNS)那么接口将自动试图与 PPPoE 服务器建立连接。如果您配置接口未与网络连接将不能启动该选项。

5.3.1 配置接口支持动态 DNS 服务

内容

启动或终止 DDNS 服务的更新。当 ZXSEC US 设备有静态的域名与动态的公共 IP 地址时，点击"启动 DDNS"使设备在每次 IP 地址更改时更新 DDNS 服务器。相应的，DDNS 服务更新具有新 IP 地址的域。

动态 DNS 只有在 NAT/路由模式下可用。

进入系统管理>网络>接口。点击"新建"或现有接口对应的编辑图标。在"寻址模式"选项栏之下启动 DDNS，并使用从 DDNS 服务器获取的信息配置 DDNS 服务。

如果 ZXSEC US 设备连接不到 DDNS 服务器，将在一分钟间隔内重试三次之后改为在三分钟的重试间隔。这样为了避免造成 DDNS 服务器增溢。

地址模式

自定义 DHCP PPPoE

IP地址/网络掩码: 0.0.0.0/0.0.0.0

DDNS 启用

Ping服务器 启用

管理访问 HTTPS PING HTTP SSH SNMP TELNET

图5.3-2 DDNS 服务配置

服务器 选择应用一个 DDNS 服务器。ZXSEC US 固件中嵌入了这些服务的客户端软件。ZXSEC US 设备能够自动与 DDNS 服务器连接。

域名 DDNS 服务器使用的域名。

用户名 与 DDNS 服务器连接使用的用户名。

密码 与 DDNS 服务器连接使用的密码。

5.3.2 配置虚拟 IPSec 接口

内容

在您进入“VPN>IPSec>自动密钥”或“VPN>IPSec>手工密钥”创建 VPN 时，可以点击“IPSec 接口模式”创建虚拟 IPSec 接口。您也可以从“本地接口列表”选择物理接口或 VLAN 接口。虚拟 IPSec 接口将在“系统>网络>接口”项下作为子接口列出。详细信息，参见“IPSec 接口模式概述”，“自动密钥”或“手工密钥”。

进入“系统>网络>接口”，点击“编辑”IPSec 接口：

- 配置 IPSec 接口的本地与远程终端的 IP 地址以便在接口应用动态路由或使用 ping 命令测试通道。
- 通过 IPSec 接口启动管理访问。
- 设置接口的日志记录。
- 输入接口的描述信息。

端口编辑

接口名称 port10 (00:09:0F:61:64:3B)

别名

虚拟域 root

地址模式

自定义 DHCP PPPoE

IP地址/网络掩码: 0.0.0.0/0.0.0.0

DDNS 启用

Ping服务器 启用

管理访问 HTTPS PING HTTP SSH SNMP TELNET

MTU 分解大于MTU的输出包, 1500 (字节)

二级IP地址

描述 (63 多个字符)

管理状态 向上 向下

确定 取消 应用

图5.3-3 虚拟 IPSec 接口设置

名称 IPSec 接口的名称。

虚拟域 选择 IPSec 接口的 VDOM。

IP/远程 IP 如果您想使用基于通道的动态路由或能够 ping 通道接口，输入本地与远程终端的 IP 地址。这两个地址不能用于网络中的其他地方。

管理访问 设置接口管理访问类型。

HTTPS 通过该接口允许到基于 web 管理器安全的 HTTPS 连接。

PING 如需要该接口对 ping 命令作出响应。使用该设置校正安装并可用于检测。

HTTP 通过该接口允许到基于 web 管理器安全的 HTTP 连接。HTTP 并不安全并且可以被第三方截取。

SSH 通过该接口允许要 CLI 的 SSH 连接。

SNMP 通过连接到该接口允许远程 SNMP 管理器请求 SNMP 信息。

TELNET 通过该接口允许到 CLI 的 Telnet 连接。Telnetl 连接并不安全并且容易被第三方截取。

描述 可选项，输入最多 63 个字符的描述信息。

5.3.3 只能使用 CLI 配置的接口

内容

几乎所有类型的接口都能够通过 GUI 的接口页面进行配置，极少数不能通过 GUI 界面配置的接口，例如回环与 VDOM 间的虚拟接口类型，只能使用 CLI 命令配置。

虚拟接口不与任何物理接口或设备之外的线缆连接。这些接口的设置可以使 ZXSEC US 设备内部进行额外的连接，实现更为复杂的配置。虚拟接口设置的另一个优点在于对速度方面如果 CPU 的负载足够虚拟接口的速度比物理接口要快。VLAN，回环接口与 VDOM 间的接口都是虚拟接口。

回环接口

回环接口是虚拟接口。设置回环接口可以协助在网络流量被丢弃时的黑洞路由（blackhole routing）。有关黑洞路由的详细信息，参见"黑洞路由"章节。

回环接口不与任何硬件连接，所以不存在硬件连接的问题。只要 ZXSEC US 设备工作正常，回环路由便是激活的。这种"永久激活"状态在很多情况下都有用途，例如动态路由。

配置回环接口的 CLI 命令称为 loop 1，IP 地址是 10.0.0.10：

```
config system interface edit loop1
    set type loopback
    set ip 10.0.0.10 255.255.255.0
  end
```

详细信息参见 ZXSEC US 设备 CLI 使用参考手册中 config system interface 命令的详细叙述。

VDOM 间的接口

虚拟域（VDOM）可以根据您的需要分流信息流量。VDOM 间的接口可以不通过物理接口将两个虚拟域连接。创建 VDOM 接口之前，必须先启动 VDOM。

通过 VDOM 间接口进行的 VDOM 之间的流量必须先要离开然后再进入通过防火墙以保持在 ZXSEC US 设备的物理接口建立的安全策略级别。

实现 VDOM 间的接口配置之前，VDOM 的设置局限于设备物理接口的数量。

VDOM 间的链接是虚拟接口，所以便不存在这样的局限。如果 ZXSEC US 设备设置了很多 VDOM，VDOM 间的接口允许您配置从单机 VDOM 配置到复杂的全网 VDOM 配置。详细信息,参见 ZXSEC US 设备 VLAN 与 VDOM 用户使用与配置手册。

创建 VDOM 间的接口时，需要配置两个终端，连接每个 VDOM。配置 VDOM 间的接口或链接接口的 CLI 命令叫 link1，将根 VDOM 连接到 vdom1：

```
config global
  config system vdom-link
    edit link1
    config system interface edit link10
    set vdom root next
    edit link11
    set vdom vdom1
    next
  end
```

详细信息，参见 ZXSEC US 设备 CLI 使用参考手册中 config system interface 命令的叙述。

接口的其他配置选项

完成所选接口的基本配置后，还可以考虑其他的配置选项，包括：

- 访问管理
- MTU 数据包容量
- 接口流量日志
- 二级 IP 地址

访问管理

运行于 NAT/路由模式下的 VDOM，您可以控制该 VDOM 中对接口的管理访问。

控制与互联网连接接口的管理访问允许处于互联网中任何地点的管理员远程管理 ZXSEC US 设备。但是，远程管理降低了 ZXSEC US 设备的网络安全性。您可以只在必需的时候配置远程管理访问，这样可以避免远程管理带来的安全性问题。

- 使用安全的管理用户密码
- 定期更改这些密码
- 启动到该接口的管理访问只使用 HTTPS 或 SSH
- 系统默认的闲置时间为 5 分钟，不做更改。

有关在透明模式下配置接口管理访问的详细信息，参见“操作模式与 VDOM 管理访问”。

设置接口的管理访问

1. 进入系统>网络>接口。
2. 选择一个接口并点击编辑图标。
3. 选择该接口的管理访问模式。
4. 点击 OK 保存配置更改。

MTU（最大传输单元）

您可以更改 ZXSEC US 设备从任何物理接口传输数据包的最大传输单元（MTU）提高网络性能。理论上，该 MTU 应该与 ZXSEC US 设备与数据包传输的目的地之间网络的最小 MTU 相同。如果 ZXSEC US 设备发送的数据包比较大，那么这些数据包就会被分拆，并减慢了传输速度。设置最佳的 MTU 可以达到最好的网络性能。

US3000 以及更高型号的设备支持巨帧。一些型号支持的最大字节是 9000，

另外一些设备是 16110 字节。巨帧的标准是最大值字节为 9000 或 16110，远远大于标准以太网帧。标准的以太网帧（数据包）包括包头信息最大可以是 1500 字节。新的以太网标准的实施（例如千兆以太网），1500 字节的帧保留作为向下的兼容。

为了通过一条路由能够发送巨帧，该路由中的所有以太网设备必须都支持巨帧，否则巨帧数据包不被识别，导致被丢弃。

如果相同的接口既有标准的以太网且有巨帧数据包流量，单独的路由并不能只根据帧容量将这些数据包路由到不同的路由线路。但是，您可以使用 VLAN 确保巨帧数据包路由到支持巨帧的网络设备。VLAN 接口的 MTU 容量与其父接口，也就是所属的接口的 MTU 容量相同。您需要配置 VLAN 包括路由线路的两端以及

路由线路上经过的所有交换机与路由器。有关 VLAN 配置的详细信息，参见 ZXSEC US 设备 VLAN 与 VDOM 用户使用与配置手册。

更改通过接口数据包的 MTU 容量

1. 进入系统>网络>接口。
2. 选择一个接口并点击编辑图标。
3. 点击“代理默认 MTU 数值（1500）”
4. 设置 MTU 容量。

如果您设置的 MTU 容量大于所配置的 ZXSEC US 设备支持的容量，系统将弹出错误信息报告。这种情况下，根据设备型号，重新输入一个相对较合适的值。MTU 支持的最大值为 16110，9000 与 1500。

注意：

如更改了 MTU,您需要重新启动 ZXSEC US 设备更新所更改接口的 VLAN 子接口的 MTU 值。

透明模式下，如果您更改了一个接口的 MTU，需要相同更改所有接口的 MTU 值与新的 MTU 值匹配。

接口流量日志

您可以对任何接口启动流量日志。详细信息，参见“流量日志”。

二级 IP 地址

对一个接口可以分配不知一个 IP 地址。您可以对接口的每个 IP 地址创建并应用单独的防火墙策略。使用二级 IP 地址，您也可以转发流量并使用 RIP 或 OSPF。

每个接口最多可以设置 32 个二级 IP 地址。一级与二级 IP 地址可以共享相同的 ping 发生器。

在您分配二级 IP 地址之前，需要考虑以下限制条件：

- 对接口必须先分配一个一级 IP 地址。
- 接口必须使用手工寻址模式。
- 默认情况下，IP 地址不能是相同子网的一部分。使用 CLI 命令可以配置允

许接口子网重叠。

```
config system global
(global)# set allow-interface-subnet-overlap enable
(global)#end
```

二级 IP 地址不能终止 VPN 通道。

您可以使用 CLI 命令 config system interface 添加接口的二级 IP 地址。详细信息，参见 ZXSEC US 设备 CLI 使用参考手册中 system interface 命令下 config secondaryip 的叙述。

二级IP地址

IP地址 / 网络掩码: 0.0.0.0/24

Ping服务器 0.0.0.0 启用

管理访问 HTTPS PING HTTP SSH SNMP TELNET

添加 /更改

#	IP地址 / 网络掩码	Ping服务器	启用Ping服务器	管理访问	

图5.3-4 添加二级 IP 地址

IP/掩码 输入 IP 地址/子网掩码。二级 IP 地址与一级 IP 地址必须在不同的子网。两个接口不能在相同的子网具有 IP 地址。只有在选择“手工寻址”模式时，该字段才可用。

Ping 服务器 启动失效网关检测，输入与接口连接的网络中下一站中继路由器的 IP 地址并点击“启动”。

管理访问 设置接口管理访问类型。

HTTPS 通过该接口允许到基于 web 管理器安全的 HTTPS 连接。

PING 如需要该接口对 ping 命令作出响应。使用该设置校正安装并可用于检测。

HTTP 通过该接口允许到基于 web 管理器安全的 HTTP 连接。HTTP 并不安全并且可以被第三方截取。

SSH 通过该接口允许要 CLI 的 SSH 连接。

SNMP 通过连接到该接口允许远程 SNMP 管理器请求 SNMP 信息。

TELNET 通过该接口允许到CLI的Telnet连接。Telnetl连接并不安全并且容易被第三方截取。添加地址后，直至点击OK或应用，所添加的二级IP地址才在列表中显示。

添加 点击“添加”在所显示的二级 IP 地址列表中添加所配置接口的二级 IP 地址。

二级 IP 地址 显示所有对接口添加的二级 IP 地址。这些地址只有在您添加地址完成后点击 OK 或应用确认后才被添加在接口中。否则一些地址因为上文所述的条件所限将从列表中删除。

\# 二级 IP 地址的编号。一个接口最多可以添加 32 个二级 IP 地址。

IP/掩码 二级 IP 地址的地址与掩码。

Ping 服务器 Ping 服务器的 IP 地址。多个二级 IP 地址可以分享一个 Ping 服务器。Ping 服务器是可选项。

启动 如果设置 ping 服务器选项，该功能框呈被选状态。

访问 对地址设置管理访问方式。二级 IP 地址之间可以设置不同的管理访问方式。

删除图标点击删除该二级 IP 地址条目。

注意：

添加二级 IP 地址后,建议返回到二级 IP 地址列表查看所添加的地址是否在地址列表中显示。如果没有显示，说明是上文所述的条件限制了地址的添加。

5.3.4 区域

内容

使用区域可以将相关联的接口与 VLAN 子接口划分为组进行管理。将接口与子接口分组管理简化了策略的创建。如果在区域中将接口与子接口分组；相比对每个

接口与 VLAN 配置连接，在区域中对一个组的接口与子接口进行统一的连接配置即可。

您可以在区域列表中添加区域，更改区域的名称、编辑及删除区域。添加区域时，选择添加到该区域的接口与接口的名称。

区域可以添加到虚拟域中。如果 ZXSEC US 配置中添加了多个虚拟域，在添加或编辑区域之前确认配置了正确的虚拟域。

接口 区 选项

新建

名称	屏蔽本区域内的流量	接口成员	

图5.3-5 区域列表

新建 点击"新建"可以创建一个区域。

名称 名称指所添加的区域的名称。

屏蔽区域内流量 如果同一区域的接口之间流量被屏蔽时显示"是"（Yes）；显示"否"（NO）表示同一区域接口间的流量没有被屏蔽。

接口成员 添加到区域的接口名称。

区域设置图 编辑与查看图标。点击该图标对区域进行编辑或查看。

删除图标 点击该图标可以删除区域。

编辑区域

名称

屏蔽本区域内的流量.

接口成员

port10 port2

port3 port4

port5 port6

port7 port8

port9 ssl.root

确定 取消

图5.3-6 区域选项

名称 输入识别该区域的名称。

屏蔽区域内流量 点击“屏蔽区域内流量”屏蔽同一区域中接口或 VLAN 子接口之间的流量。

接口成员 选择所列接口作为该区域的一部分。该列表包括配置的 VLAN。

网络选项

网络选项包括 DNS 服务器与失效网关检测设置。

进入“系统>网络>选项”配置 DNS 服务器与失效网关检测设置。

网络选项

DNS设置

首选DNS 服务器 65.39.139.53

备选DNS 服务器 65.39.139.63

本地域名

失效网关检测

检测间隔 5 (秒)

故障恢复检测 5 (丢失连续的ping)

应用

图5.3-7 网络选项

自动获取 DNS 服务器地址 该功能项只适用于 ZXSEC US180 以及以下型号的设备。当配置接口使用 DHCP 的同时，接口将自动获取 DNS 服务器 IP 地址。该操作只适用于 NAT/路由模式。您还应该在接口的 DHCP 设置中启动“代理内部 DNS”选项。参见“配置接口使用 DHCP”。

使用以下的 DNS 服务器地址 该功能项只适用于 ZXSEC US180 以及以下型号的设备。使用指定的一级与二级 DNS 服务器地址。

一级 DNS 服务器 输入一级 DNS 服务器 IP 地址。

二级 DNS 服务器 输入二级 DNS 服务器 IP 地址。

本地域名

启动 DNS 转发网络 该功能项只适用于运行于 NAT/路由模式的 ZXSEC US180 以及以下型号设备。选择从您配置的 DNS 服务器转发 DNS 请求的接口。

失效网关检测 失效网关检测是通过在接口配置的 ping 服务器发送 ping 指令以检测连接是否畅通。有关在接口配置 ping 服务器的详细信息，参见“在接口配置 Ping 服务器”。

检测间隔 设置失效网关检测的时间间隔。输入时间（秒计）设定 ZXSEC US 设备发送 ping 包进行检测的时间间隔。

故障恢复检测 设置失效网关检测失败的次数以便 ZXSEC US 设备判定网关是否继续工作。

5.4 DNS 服务器

内容

ZXSEC US 设备的几项功能包括报警邮件及以 URL 屏蔽都需要配置 DNS 选项.您可以指定 ZXSEC US 设备连接的 DNS 服务器的 IP 地址。DNS 服务器 IP 地址通常是由您的 ISP 服务商提供的。

您可以配置 ZXSEC US180 或以下型号的设备自动获取 DNS 服务器地址。配置自动获取 DNS 地址，您至少配置一个接口使用 DHCP 或 PPPoE 寻址模式。参见“配置接口使用 DHCP”或“配置接口使用 PPPoE”。

ZXSEC US180 或该型号以下的设备可以在接口配置 DNS 转发功能。所属网络中的主机将使用该接口的 IP 地址作为其 DNS 服务器。发送到接口的 DNS 请求将被转发在您配置的或 ZXSEC US 设备自动获取的 DNS 服务器地址。

失效网关检测

失效网关检测就是定期发送 ping 指令到一个 ping 服务器确认连接是否正常。典型的网络配置是 ping 服务器是通向外部网络或互联网的下一跳路由。检测间隔与失效 ping 的数量是衡量连接性的指标您可以进入系统管理>网络>选项中配置失效网关检测选项。在接口应用失效网关检测时您必须对接口配置一个 Ping 服务器。

在接口添加 **ping** 服务器

1. 进入“系统>网络>接口”。
2. 选择一个接口并点击“编辑”。
3. 将 Ping 服务器设置为与该接口连接的下一跳路由的 IP 地址。
4. 选中“启动”功能框。
5. 点击 OK 保存配置更改。

路由表（透明模式）

透明模式下，进入“系统>网络>路由表”，配置添加从 ZXSEC US 设备到本地路由器的静态路由。

新建

IP/掩码	网关	设备	路径长度	
0.0.0.0/0.0.0.0	10.16.13.3	port2	10	
0.0.0.0/0.0.0.0	0.0.0.0	port2	10	

图5.4-1 路由列表

新建 点击“新建”添加新的路由。

路由序号。

IP 该路由的目标 IP 地址。

掩码 该路由的掩码。

网关 该路由指向的下一个路由的 IP 地址。

管理距离 相对可信的路由。1 表示最值得信赖的路由。

删除图标， 点击该图标删除一个路由。

查看/编辑图标， 点击该图标查看或编辑一个路由。

移动图标， 点击该图标可以更改路由在列表中的顺序。

透明模式下的路由设置

进入“系统>网络>路由表”，点击“新建”添加路由。您也可以点击现有路由对应的编辑图标对其进行修改。

新建路由

目的 IP/掩码	0.0.0.0/0.0.0.0
网关	0.0.0.0
管理距离	10 (1-255)

确定 取消

图5.4-2 透明模式下的路由选项

目的 IP 地址与掩码 输入该路由的目的地 IP 地址与掩码。

网关　　输入该路由指向的下一跳路由的 IP 地址。对于一个互联网连接，下一跳路由网关的流量到互联网。

管理距离　　相对可信的路由。1 表示最值得信赖的路由。

配置调制解调器接口

US70 系列与 US120 系列设备配有调制解调器，您可以使用调制解调器在 NAT/路由模式下作为一个备用接口或单机接口。

- 冗余模式（备份模式）下，当以太网接口不可用时调制解调器接口将自动取代该接口进行工作。
- 单机模式下，调制解调器接口是 ZXSEC US 设备与互联网之间的连接。

与 ISP 建立连接时，ZXSEC US 设备调制解调器能够自动对拨号三个帐户直至与一个 ISP 建立连接。

US70AM 与 US120AM 有内置的调制解调器。对于这两个型号的设备，您可以在基于 web 管理器中配置调制解调器的操作。参见“配置调制解调器的设置”。

其它 US70AM 与 US120AM 设备可以通过一个 USB 到串口的转换器与外部的调制解调器连接。对于这些型号的设备，您必须使用 CLI 配置调制解调器的操作。参见 ZXSEC US 设备 CLI 使用参考手册中有关 system modem 的命令描述。

**注意：**

调制解调器接口不是用于远程 console 连接的 AUX 端口，它没有相关联的接口。ZXSEC US2010，2010A 与 ZXSEC US2350A 支持 AUX 端口。详细信息，参见 ZXSEC US 设备 CLI 使用参考手册中有关 system aux 的命令描述。

配置调制解调器设置

配置调制解调器设置，以便 ZXSEC US 设备可以使用调制解调器与您的 ISP 拨号帐户连接。您最多可以配置三个拨号帐户，选择冗余或单机操作模式以及配置拨号方式。

只有在 NAT/路由模式下可以配置使用调制解调器。

启动调制解调器　选中该功能框启动调制解调器设置。

调制解调器的状态　　其状态表现为“未激活”、“正在连接”、“已连接”、“断开连接”或是“挂断”其中的一种。（只适用于单机模式）

拨号/挂断 （只适用于单机模式）点击“拨号”自动与拨号帐户建立连接。连接建立后，您也可以点击“挂断”自动断开与调制解调器的连接。

冗余接口 （只适用于冗余模式）选择以太网接口，调制解调器可以提供后备服务。

随需拨号 （只适用于单机模式）当数据包路由到调制解调器接口时点击选择拨号调制解调器。

闲置超时 （只适用于单机模式）输入超时时间。在设定的超时时间段内没有网络活动，将自动断开连接。

等候计时 （只适用于冗余模式）设置从调制解调器接口切换到主接口之前，主接口恢复之后 ZXSEC US 设备等待的时间。如果您发现 ZXSEC US 设备在主接口与调制解调器接口之间频繁切换的时候，设置稍长的等待时间。

重拨限次 如果调制解调器试图与 ISP 的拨号连接失败后，重新拨号的最大次数。默认的最大重拨次数是 1。选择“无”表示重拨不限次。

拨号帐户 最多可以配置三个拨号帐户。ZXSEC US 设备依次连接各个帐户直至连接建立。

电话号码 连接拨号帐户所需的电话号码。电话号码之间不能有空格。根据拨号帐户设置要求填写所需信息。

用户名 发送到 ISP 的用户名。（最多 63 个字符长度）

密码 发送到 ISP 的密码。

有关冗余模式下配置调制解调器，参见“冗余模式配置”。

有关单机模式下配置调制解调器，参见“单机模式配置”。

5.5 冗余模式配置

内容

调制解调器接口在冗余模式下备份作为可选的以太网接口。如果以太网接口从网络断开，调制解调器将自动承接拨号配置的拨号帐户的任务。当调制解调器连接到拨号帐户，ZXSEC US 设备将到达已选以太网接口的数据包路由到调制解调器接口。

当以太网接口能够重新与其网络连接时，ZXSEC US 设备将断开与调制解调器接口的连接切换恢复到以太网接口。您可以设置“等候计时”拖延切换回以太网接口以便在通信之前能确保网络连接的稳定。

“闲置超时”是可选项，在设定的超时时间段内没有网络活动，将自动断开连接。能够节省拨号连接的费用。

如果使 ZXSEC US 设备能够从以太网接口切换到 modem 接口，您必须在 modem 配置中选择一个接口，并对该接口配置 ping 服务器设置。您也必须对 modem 接口与其他 ZXSEC US 接口之间的连接配置防火墙策略。

注意：

不要对 modem 接口与作为 modem 接口备用接口之间的连接添加任何防火墙策略。

配置冗余模式

1. 进入“系统>网络>Modem”。
2. 选择“冗余模式”。
3. 配置输入以下信息：

模式 冗余模式

备用接口从列表中选择作为备用的接口。

等候时间输入在接口恢复连接后继续使用 modem 的时间。（以秒计）

重拨限次如果 ISP 没有回应，重试连接的最多限次。

拨号帐户 1 最多可以设置三个 ISP 帐户，分别输入电话号码、用户名与密码。

拨号帐户 2

拨号帐户 3

4. 点击“应用”。
5. 对以 modem 接口作为备份的以太网接口配置 ping 服务器。参见“在接口添加 ping 服务器”。
6. 对到 modem 接口的连接配置防火墙策略。参见“对 modem 连接添加防火墙策略”。

单机模式配置

单机模式下，通过 modem 可以与互联网连接。您可以配置 modem 在 ZXSEC US 设备在重启时或没有路由的数据包时进行拨号连接。您也可以手动挂断 modem 拨号连接或重新进行拨号连接。

如果与拨号帐户的连接失败，ZXSEC US 设备将重拨 modem。重播限次中可以设定 modem 重拨的最多次数，或直至连接建立。

“闲置超时”是可选项，在设定的超时时间段内没有网络活动，将自动断开连接。能够节省拨号连接的费用。

对于 modem 接口与其它 ZXSEC US 接口之间的连接，必须配置防火墙策略。

进入“路由器>静态路由”配置静态路由将流量路由到 modem 接口。例如，如果 modem 接口配置作为 ZXSEC US 设备的外部接口，您必须配置“接口设置”将默认路由设置到 modem。

单机模式下的操作

1. 进入“系统>网络配置>Modem”。
2. 配置输入以下信息：

模式　　单机模式

自动拨号　　选中该功能框，如果您设置在 ZXSEC US 设备重启时自动进行 modem 连接。

随需拨号设置每当存在没有路由的数据包时 modem 与 ISP 连接。

闲置超时　　输入闲置超时的时间。（以分钟计）在超出设定的时间内没有任何网络活动，自动断开连接。

重拨限次　　如果 ISP 没有回应，重试连接的最多限次。

拨号帐户 1　　最多可以设置三个 ISP 帐户，分别输入电话号码、用户名与密码。

拨号帐户 2

拨号帐户 3

3. 点击“应用”。
4. 对到 modem 接口的连接配置防火墙策略。参见“给 modem 连接添加防火墙策略”。

5. 进入“路由器>静态路由”配置静态路由将流量路由到 modem 接口。给 modem 连接添加防火墙策略。

对 modem 连接添加防火墙策略

Modem 接口需要添加防火墙地址与策略。在 modem 接口，您可以添加一个或更多个地址。有关添加地址的详细信息，参见“配置地址”。地址添加完成后，modem 接口显示在策略网格中。

您可以配置防火墙策略控制 modem 接口与 ZXSEC US 设备其他接口之间的数据包流。有关添加防火墙策略的详细信息，参见“添加防火墙策略”。

配置建立或断开与 modem 的连接

Modem 必须配置在单机模式下。与拨号帐户连接

1. 进入“系统>网络配置>Modem”。
2. 点击“启动 USB Modem”。
3. 确定拨号帐户的信息填写正确。
4. 如果做了其他配置的更改，点击“应用”。
5. 点击“拨号”。

ZXSEC US 设备发起与每个帐号的连接，直至连接成功。

断开连接

使用以下步骤断开 modem 与拨号帐户的连接。

1. 进入“系统>网络配置>Modem”。
2. 点击“挂断”可以中断与拨号帐户的连接。

查看 modem 的状态

您可以查看 modem 的连接状态，以及哪个拨号帐户处于激活状态。如果 modem 与 ISP 建立了连接，您可以看到 IP 地址与掩码。

进入“系统>网络配置>Modem”，可以查看 modem 的状态。

Modem 的状态显示为以下其中之一：

未激活　Modem 没有与 ISP 建立连接。

已连接　Modem 与 ISP 连接成功。

连接中　Modem 正在与 ISP 建立连接。

断开连接 Modem 与 ISP 断开连接。

挂断 断开从 modem 到 ISP 的连接。（只适用于单机模式）

点击“连接”modem 将重新拨号建立与 ISP 的连接。

检查标记呈绿色表示帐户已激活。

分配到 modem 接口的 IP 地址与掩码将在基于 web 管理器的系统网络接口页面中显示。

5.6 VLAN 概述

描述

一个 VLAN 是一组相互发生通讯计算机，服务器与其它网络设备在逻辑上处于同一个 LAN 网段的划分，即使这些设备在物理上并不属于同一网段。例如，为会计部门工作的的工作站与服务器可以分布在办公区的不同位置，并与众多网段连接，但是他们仍然可以处于同一个 VLAN 中。

VLAN 是将 LAN 设备从逻辑上而不是物理上划分为一个网段。每一个 VLAN 都可作为一个广播域。处于 VLAN 1 中的设备可以与处于 VLAN 2 中的设备连接，但是不能够与其它 VLAN 中的设备连接。VLAN 之间的设备通讯在物理位置可以处于独立的不同区域，但是逻辑上处于同一 VLAN。

一个 VLAN 是通过在 VLAN 中的设备发送与接收的数据包添加 802.1Q 帧标签进行设备划分的。VLAN 标签是 4byte 的帧扩展，包含一个 VLAN 标识符及其它信息。

VLAN 的应用增强了网络的管理灵活性，减少了设备投资提高了网络的安全性。

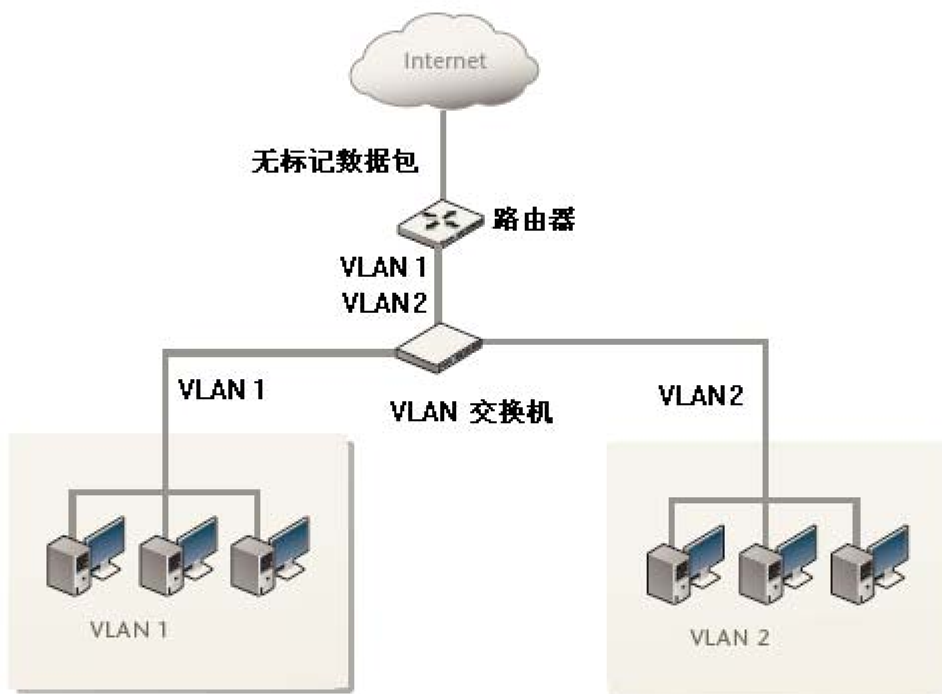


图5.6-1 基本的 VLAN 拓扑结构

5.6.1 ZXSEC US 设备与 VLAN

内容

在典型的 VLAN 配置中，在通过 802.1Q 的 VLAN2 层的交换机或 3 层的路由器或防火墙的数据包上添加 VLAN 标签。2 层的交换机能够处理同一 VLAN 设备通过的数据包。不同 VLAN 之间的设备通讯数据包只能够被 3 层的设备如路由器，防火墙与 3 层的交换机处理。

使用 VLAN，一个单一的 US 设备既能够提供安全性服务又能够控制多个安全域之间的连接。从每个安全域流出的流量都标有不同的 VLAN ID。ZXSEC US 设备可以识别 VLAN ID 并应用安全性策略确保安全域之间可信的网络与 IPSecVPN 流量。ZXSEC US 设备也可以对通过安全域之间的网络与 VPN 流量应用安全性验证，保护设置以及其它防火墙策略功能。

5.6.2 NAT/路由模式下配置 VLAN

内容

NAT/路由模式下，ZXSEC US 作为 3 层设备控制多个 VLAN 之间的数据包流。

ZXSEC US 设备也可以删除向内的 VLAN 数据包的 VLAN 标签并将没有标签的数据包转送到其它网络，如互联网。

NAT/路由模式下，ZXSEC US 设备支持 IEEE 802.1Q 交换机（或路由器）与 ZXSEC US 设备之间创建 VLAN trunk。

通常情况下，通过在内部交换机上与 VLAN Trunk 连接的 ZXSEC US 内部接口与下行 Internet 路由器连接的外部接口的流量没有被标注。ZXSEC US 设备可以应用不同的防火墙策略对与内部接口连接的通过每个 VLAN 的流量进行控制。

该配置下，对 ZXSEC US 内部接口添加 VLAN 子接口设置接口的 VLAN ID 与 VLAN trunk 中数据包的 VLAN ID 相同。ZXSEC US 设备将与子接口 VLAN ID 相匹配的数据包发送到该子接口。

您可以在 ZXSEC US 设备所有的接口上定义 VLAN 子接口。ZXSEC US 设备可以在通过 VLAN 子接口的数据包上添加 VLAN 标签，或从流入的数据包中删除 VLAN 标签并同时在流出的数据包上添加不同的 VLAN 标签。

VLAN ID 设置规则

NAT/路由模式下，添加到同一物理接口的两个 VLAN 子接口不能拥有相同的 VLAN ID。但是，您可以在不同的物理接口上添加两个或更多的 VLAN 子接口使用相同的 VLAN ID。拥有相同 VLAN ID 的两个 VLAN 子接口之间没有内部连接或链接。他们之间的关系与任何两个 ZXSEC US 网络接口之间的关系相同。

VLAN IP 地址设置规则

所有 ZXSEC US 设备接口的 IP 地址都不能够重叠。也就是说，所有接口的 IP 地址都属于不同的子网。该规则适用于物理接口与 VLAN 子接口 IP 设置。

注意：

如果您不能更改现行的配置避免 IP 地址的重叠输入 CLI 命令 config system global 与 set ip-overlap enable 允许 IP 地址重叠。输入以上命令后，多重的 VLAN 接口可以使用与其它接口 IP 地址相重叠某一部分的 IP 地址。建议最好是高级用户使用该命令。

简化的 NAT/路由模式 VLAN 配置。该示例中，与 VLAN 交换机连接的 ZXSEC US 内部接口使用 802.1Q trunk 并配置了两个 VLAN 子接口（VLAN100 与 VLAN200）。外部接口与互联网连接。外部接口不配置 VLAN 子接口。

当 VLAN 交换机从 VLAN100 与 VLAN200 接收数据包时，标注 VLAN 标签并将数据包转送到本地接口通过 trunk 到 ZXSEC US 设备。ZXSEC US 配置使用了策略允许通过 VLAN 之间的数据流以及从 VLAN 到外部网络的数据传输。

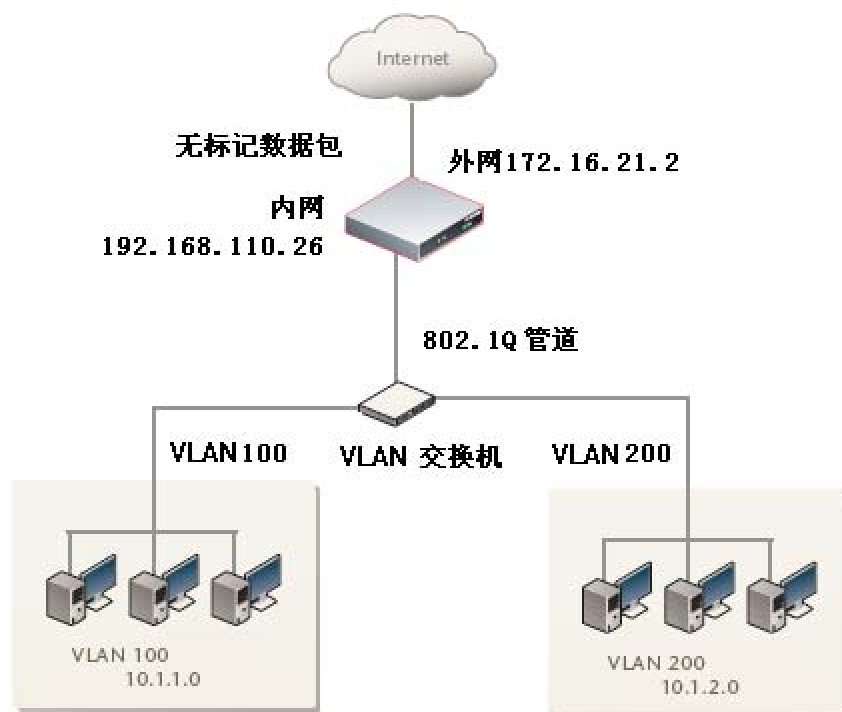
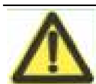


图5.6-2 运行于 **NAT**/路由模式的 **ZXSEC US** 设备

添加 VLAN 子接口

每个 VLAN 子接口的 VLAN ID 必须与 IEEE 802.1Q 路由器添加 VLAN ID 相匹配。

VLAN ID 可以为 1 到 4096 之间任何的数字。每个 VLAN 子接口也必须配置各自的 IP 地址与掩码。

注意：

一个 VLAN 不可以与虚拟域或区域具有相同的名称。在物理接口添加 VLAN 子接口接收标有 VLAN 标签的数据包。

NAT/路由模式下添加 VLAN 子接口

1. 进入“系统>网络配置>接口”。

2. 点击“新建”添加 VLAN 接口。

3. 输入能够识别 VLAN 接口的名称。

4. 选择通过该 VLAN 子接口接收 VLAN 数据包的物理接口。

5. 输入与该 VLAN 子接口接收到的数据包的 VLAN ID 相匹配的 VLAN ID。

6. 如果您使用超级管理员帐户登录，选择添加该 VLAN 子接口的虚拟域。否则，您只能在所属的 VDOM 创建 VLAN 子接口。有关虚拟域信息，参见“虚拟域”。

7. 配置 VLAN 子接口的方法类似 ZXSEC US 接口的配置。

8. 点击 OK 保存配置更改。

重复步骤 4，可以在 ZXSEC US 设备的物理接口继续添加 VLAN 子接口。

5.6.3 给 VLAN 子接口设置防火墙策略

内容

添加了 VLAN 子接口后，可以给 VLAN 子接口之间的连接或从一个 VLAN 子接口到物理接口的流量添加防火墙策略。

1. 进入“防火墙>地址”。

2. 点击“新建”添加防火墙地址，与 VLAN 数据包的源及目标地址相匹配。

3. 进入防火墙>策略。

4. 根据需要添加防火墙策略。

透明模式下配置 VLAN

透明模式下，ZXSEC US 可以在 IEEE 302.1VLAN 上应用防火墙的策略和服务，例如认证、保护设置以及其它防火墙功能。您可以将运行于透明模式的 ZXSEC US 设备安插到一个 VLAN 中，不做任何的网络设置修改。典型的应用配置是，ZXSEC US 的内部接口接收来自内部 VLAN 连接的 VLAN 交换机或路由器的数据包。ZXSEC US 的外部接口将没有 VLAN 标签的数据包转送到与互联网连接的外部 VLAN 交换机或路由器。对于每项 VLAN 中的数据流量，ZXSEC US 可以配置使用不同的策略。

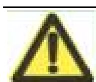
对于 ZXSEC US 设备内部与外部接口之间的数据传输，您可以在内部接口上添加 VLAN 子接口以及在外部接口添加其它的 VLAN 子接口。如果这些添加的 VLAN 子接口使用相同的 VLAN ID，ZXSEC US 设备可以对该 VLAN 中的通讯数据包应

用防火墙策略。如果这些 VLAN 子接口使用不同的 VLAN ID，或者添加了多于两个的 VLAN 子接口，您也可是使用防火墙策略控制 VLAN 之间的连接。

如果使用 IEEE 802.1VLAN 标签划分网络流量，您可是配置运行于透明模式的 ZXSEC US 设备控制通过不同 VLAN 之间流量的安全性。支持透明模式下的 VLAN 传输，您可以在 ZXSEC US 设备配置中添加虚拟域。一个虚拟域由两个或更多的 VLAN 子接口或区域组成。在一个虚拟域中，一个区域能够包括一个或多个 VLAN 接口。

当 ZXSEC US 设备的一个接口接收到标有 VLAN 标签的数据包时，该数据包将被发送到与 VLAN I 相匹配的 VLAN 子接口。VLAN 子接口删除 VLAN 标签并根据其目的地 MAC 地址分配数据包所要到达的目的地接口。对源与目标地址为 VLAN 子接口的数据包应用该防火墙策略。

如果数据包是防火墙接收到的，ZXSEC US 设备将数据包转送到目的 VLAN 子接口。ZXSEC US 将给数据包加上目的地 VLAN ID 并将数据包发送到 VLAN。

注意：

透明模式下，每个 VDOM 允许配置最多 255 个接口，包括 VLAN。如果一个 VDOM 中没有配置任何其它接口，您可以在 VDOM 内最多配置 255 个 VLAN。

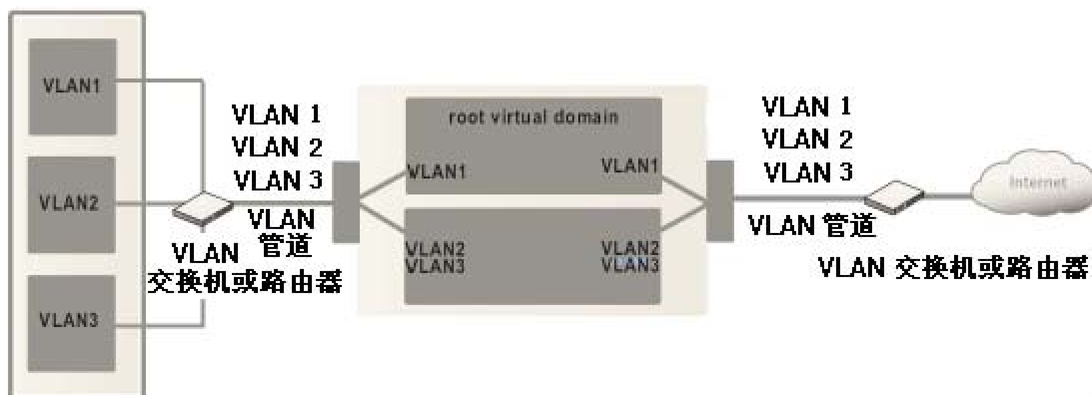


图5.6-3 透明模式下配置有两个虚拟域的 ZXSEC US 设备

透明模式下配置有三个 VLAN 子接口的 ZXSEC US 设备。该配置中，ZXSEC US 设备安置在网络中为每个 VLAN 提供病毒扫描，网页内容过滤以及其它服务的网络安全设备。

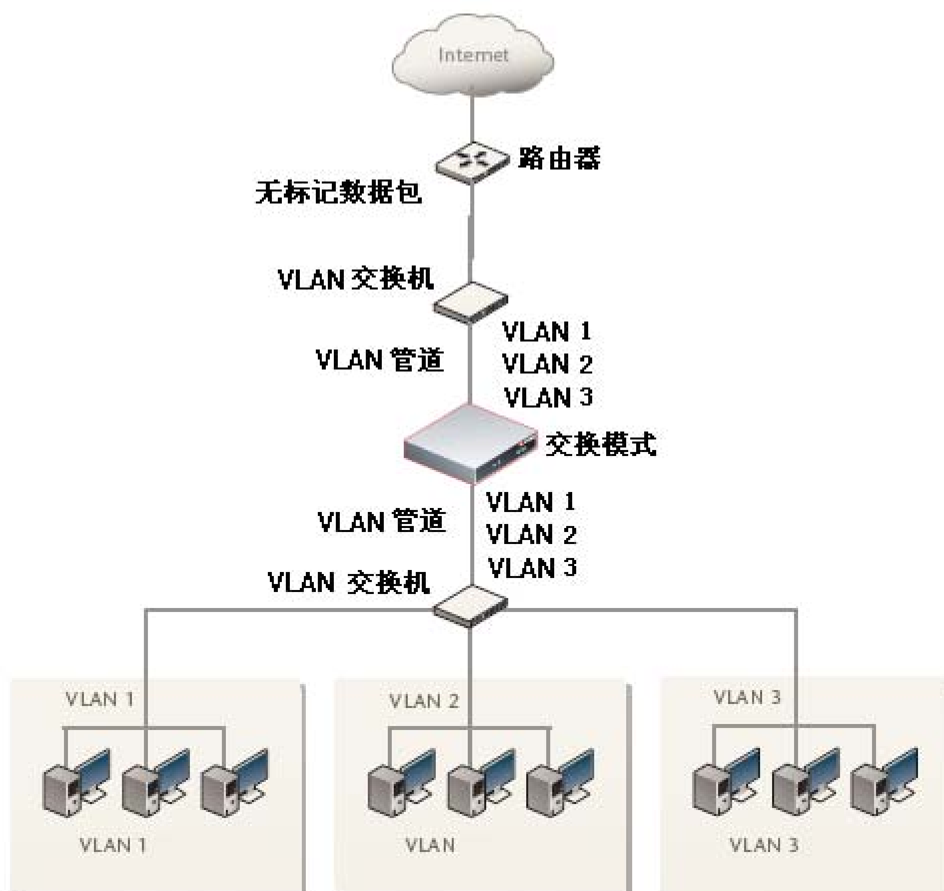


图5.6-4 透明模式下 ZXSEC US 设备

VLAN ID 设置规则

透明模式下,添加到同一物理接口的两个 VLAN 子接口不能拥有相同的 VLANID。但是,您可以在不同的物理接口上添加两个或更多的 VLAN 子接口使用相同的 VLAN ID。拥有相同 VLAN ID 的两个 VLAN 子接口之间没有内部连接或链接。他们之间的关系与任何两个 ZXSEC US 网络接口之间的关系相同。

注意:

透明模式下,每个 VDOM 允许配置最多 255 个 VLAN。

5.6.4 透明模式下设置虚拟域与 VLAN

内容

添加 VLAN 子接口以及虚拟域。默认情况下，ZXSEC US 配置包括一个虚拟域，叫做 root。您可以根据需要在该虚拟域中添加 VLAN 子接口。

如果想将 VLAN 子接口组划分到虚拟域中，您可以添加更多的虚拟域。

透明模式下添加 **VLAN** 子接口

每个 VLAN 子接口的 VLAN ID 必须与 IEEE 802.1Q 路由器或交换机添加的 VLANID 相同。VLAN ID 可以设置为 1 到 4096 之间的任何数字。您可以在物理接口上添加 VLAN 子接口接收标有 VLAN 标签的数据包。

注意：

VLAN 不能与虚拟域或区域同名。

---

1. 进入"系统>网络>接口"。
2. 点击"新建"添加 VLAN 接口。
3. 输入 VLAN 子接口的名称。
4. 选择通过该 VLAN 子接口接收 VLAN 数据包的物理接口。
5. 输入与该 VLAN 子接口接收到的数据包的 VLAN ID 相匹配的 VLAN ID。
6. 选择该 VLAN 子接口所属的虚拟域，有关虚拟域信息，参见"虚拟域"。
7. 配置 ZXSEC US 任何接口的管理访问与日志设置。有关这些设置的详细信息，参见"接口设置"。
8. 点击 OK 保存配置更改。ZXSEC US 设备便在接口添加新的子接口。
9. 点击"启动"启动 VLAN 子接口。

给 **VLAN** 子接口添加防火墙策略

完成 VLAN 子接口的添加后，您能够添加防火墙策略对子接口间的连接或从 VLAN 子接口到物理接口之间的流量进行控制。

1. 进入"防火墙>地址"。

2. 点击“新建”添加防火墙地址与 VLAN 数据包的源以及目标 IP 地址相匹配。参见“防火墙地址”。

3. 进入“防火墙>策略”。

4. 根据需要添加防火墙策略。

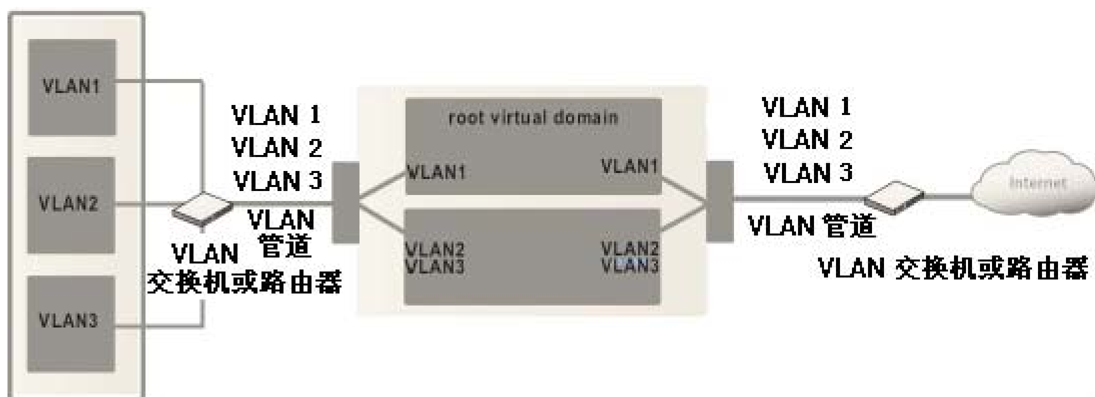


图5.6-5 配置了两个虚拟域的 ZXSEC US 设备运行于透明模式

透明模式下配置有三个 VLAN 子接口的 ZXSEC US 设备。该配置中，ZXSEC US 设备安置在网络中为每个 VLAN 提供病毒扫描，网页内容过滤以及其它服务的网络安全设备。

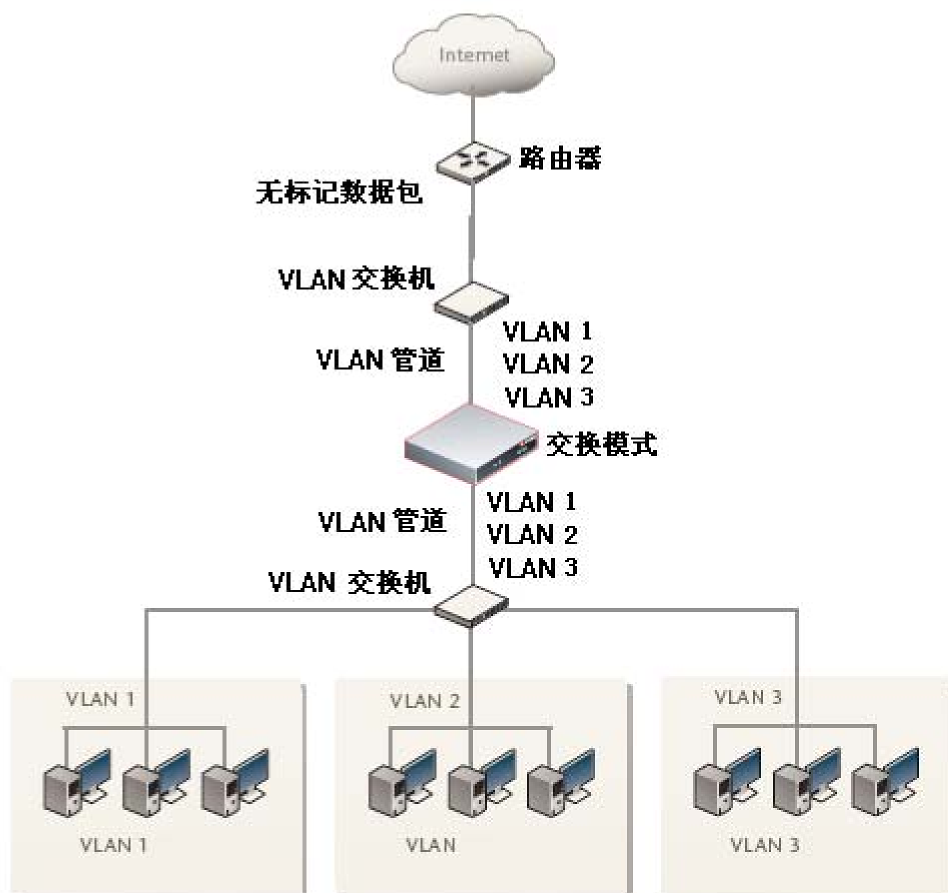


图5.6-6 运行于透明模式下的 ZXSEC US 设备

有关 ARP 的故障诊断与检修

地址解析协议（ARP）对于网络的通信至关重要，且默认在接口中启动。通常情况下，ARP 数据包被允许通过 ZXSEC US 设备，特别是用户端与服务器或用户端与路由器之间的 ARP 数据包。

复制 ARP 数据包

ARP 流量会导致一些问题，尤其是在透明模式下当 ARP 数据包到达将要被发送到所有其它接口的一个接口，包括到达 VLAN 子接口。一些第二层网络交换机设备在检测到相同的 MAC 地址从不止一个接口或从多个 VLAN 中发出时便会变得不稳定。不稳定的原因在于二层交换机设备没有对每个 VLAN 保持独立的 MAC 地址列表。不稳定状态下的交换机可能会重新启动，导致流量传输缓慢。

ARP 转发针对以上情况，方案之一便是启动 ARP 转发。ARP 转发可以使用 GUI 或 CLI 进行配置。GUI 中，进入“系统>配置>操作”启动 ARP 转发。有关在 CLI 中配置 ARP 转发的详细信息，参见 ZXSEC US 设备 CLI 使用参考手册。

ARP 转发启动后，ZXSEC US 设备将允许复制 ARP 数据包便解决了上述的问题。但是启动 ARP 转发同时也带来可能的欺骗数据包对网络的攻击有关的更详细的安全解决方案，参见 ZXSEC US 设备备 VLAN 与 VDOM 用户使用与配置手册。

5.6.5 ZXSEC US 支持 IPv6

内容

对 **ZXSEC US** 设备任何接口的地址分配既可以是 IPv4 又可以是 IPv6。接口的功能形象化划分作为两个接口：一个接口用来处理 IPv4 地址的数据包，另一个接口用来处理 Ipv6 地址的数据包。

ZXSEC US 设备支持 IPv6 路由、通道、防火墙策略与 IPSec VPN。您必须使用 CLI 配置 IPv6 的操作。详细信息，参见中兴通讯公司网页知识库板块中有关 USIPv6 技术手册中叙述。

有关以下命令，参见 US 设备 CLI 使用参考手册。

功能	CLI 命令
接口配置，包括定期路由器广播	config ststen interface config ip6-profix-list
静态路由	config router static6
IPv6 隧道	config system ipv6_tunnel
IPv6 IPSec VPN	config vpn ipsec
执行	execute ping6
防火墙	config firewall address6 config firewall addrgrp6 config firewall policy6

第6章 配置使用 DHCP

6.1 概述

描述

本章是关于如何使用 DHCP 为用户提供便捷的自动网络配置服务的内容描述。

内容

本章内容如下：

6.2 US DHCP 服务器与中继代理

内容

DHCP 协议可以使主机自动获取分配的 IP 地址。或者也可以获取默认的网关与 DNS 服务器设置。一个 ZXSEC US 接口或 VLAN 子接口能够提供以下 DHCP 服务：

- 为常规以太网连接提供常规的 DHCP 服务器服务。
- 为 IPSec（VPN）连接提供 IPSec DHCP 服务器服务。
- 为常规以太网或 IPSec 连接提供 DHCP 中继服务。

对于相同类型的连接（常规或 IPSec），一个接口不能既提供 DHCP 服务器服务又提供中继代理服务。

注意：

只有当接口配置使用静态 IP 地址时您可以对接口配置一个常规 DHCP 服务器。

您可以对使用静态或动态地址的接口配置 IPSec DHCP 服务器。

您可以对任何 ZXSEC US 接口配置 DHCP 服务器功能。DHCP 服务器对与该接口连

接的网络中的主机动态分配 IP 地址。在主机上必须配置使用 DHCP 自动获取分配的 IP 地址。

如果一个接口通过路由器与多个网络连接，您可以对每个网络添加一个 DHCP 服务器。每个 DHCP 服务器的 IP 地址范围必须与网络地址范围相匹配。路由器必须配置使用 DHCP 中继代理。

有关配置 DHCP 服务器信息，参见“配置 DHCP 服务器”。

ZXSEC US 接口可以配置作为 DHCP 中继代理.接口将 DHCP 用户端的 DHCP 请求转发到外部 DHCP 服务器并将回应返回到 DHCP 用户。DHCP 服务器必须具有适当的路由，以便返回到 DHCP 用户的回应数据包能够到达 ZXSEC US 设备。有关配置 DHCP 中继的信息，参见“配置接口作为 DHCP 中继代理”。

使用 CLI 也可以配置 DHCP 服务器。

6.3 配置 DHCP 服务

内容

进入“系统>DHCP>服务”，配置接口的 DHCP 服务。您可以配置每个接口执行 DHCP 中继代理与添加 DHCP 服务器。

US70 与 US120 设备中，DHCP 服务器是已经配置好的。默认的情况下，是配置在内部接口上，配置信息如下：

IP 地址范围　192.168.1.110 到 192.168.1.210

掩码　　255.255.255.0

默认网关　　192.168.1.99

租期　　7 天

DNS 服务器 1　　192.168.1.99

您可以撤消或更改默认的 DHCP 服务器配置。以上设置适用于默认内部（Internal）接口 IP 地址 192.168.1.99。如果您将该地址更改为不同网络的地址，您需要更改相应得 DHCP 服务器与之相匹配。

接口	服务器名称/中继IP	类型	启动	
loop1				
中继	-	-		
服务器	-	-		
port1				
中继	-	-		
服务器	-	-		
port10				
port2				
port3				
port4				
port5				
port6				
port7				
port8				
port9				

图6.3-1　**DHCP** 服务列表

接口　　ZXSEC US 接口列表点击所列接口左边的蓝色三角图标可以扩展查看中继与服务器。

服务器名称/中继 IP　　US DHCP 服务器名称或中继访问的 DHCP 服务器的 IP 地址。

添加 DHCP 服务器图标　　对该接口配置与添加 DHCP 服务器。

编辑图标　　点击该图标可以查看或修改接口配置的中继或 DHCP 服务配置。

删除图标　　删除 DHCP 服务器。

6.3.1 配置接口作为 DHCP 中继代理

内容

进入“系统>DHCP>服务”，点击每个接口对应的编辑图标查看或修改 DHCP 中继配置。

编辑DHCP中继设置

接口名称　loop1

DHCP中继代理　☐ 启动

类型　◉ 经常　○ IPSEC

DHCP服务器IP

OK　取消

图6.3-2　给接口配置 **DHCP** 中继设置

接口名称　　接口的名称。

启动　　在该接口中启动 DHCP 中继代理。

类型　　选择 DHCP 服务的类型。配置接口作为与该接口连接的网络中的计算机的 DHCP 中继代理。

IPSec　　配置接口只作为与该连接发生的 IPSec VPN 连接的远程 VPN 用户的中继代理。

DHCP 服务器 IP 地址　输入 DHCP 服务器的 IP 地址，该服务器用于对与该接口连接的网络中的计算机作出 DHCP 回应。

6.3.2 配置 DHCP 服务器

内容

进入“系统>DHCP>服务”，可以配置接口的 DHCP 服务器。点击接口旁边的“添加 DHCP 服务器”或点击现有 DHCP 服务器对应的编辑图标更改设置。

新建DHCP服务器
名称
启动
类型　经常　IPSEC
IP范围　0.0.0.0 - 0.0.0.0
掩码　0.0.0.0
缺省网关
域
租期　无限
7 (天) 0 (小时) 0 (分钟)
(5 分钟 - 100 天)
高级… (DNS、WINS、自定义选项、排除范围。)
OK　取消

图6.3-3　服务器选项

名称　　输入 DHCP 服务器的名称。

启动　　选中该功能框启动 DHCP 服务器设置。

类型 选择常规或 IPSec DHCP 服务器类型。

您不能在使用动态 IP 地址的接口配置常规 DHCP 服务器。

IP 范围 输入 DHCP 服务器分配给 DHCP 用户的开始与终止 IP 地址范围。

掩码 输入 DHCP 分配给 DHCP 用户的掩码。

缺省网关 输入 DHCP 服务器分配 DHCP 用户的默认网关地址。

域 输入 DHCP 服务器分配给 DHCP 用户的域名。

租期 选择无限制租用时间或是限定租用时间。租用时间过期后DHCP 用户必须向 DHCP 服务器要求新的设置.租用时间的范围可以设置为 5 分钟到 100 天之间的任何时间段。

高级选项 点击配置高级选项。

DNS 服务器 1 输入 DHCP 服务器分配给 DHCP 客户的最多 3 个 DNS 服务器的 IP 地址。

DNS 服务器 2

DNS 服务器 3

WINS 服务器 1 添加 DHCP 服务器分配给 DHCP 用户的一个或两个 WINS 服务器的

WINS 服务器 2 IP 地址。

选项 1 DHCP 服务器最多能够发送三个自定义 DHCP 选项。代码是 1 到 255 之间的 DHCP 选项代码。选项是 16 进制字符的偶数，一些选项代码并不要求。有关 DHCP 选项的详细信息，参见 RFC2132 DHCP Options and BOOTP Vendor Extensions。

选项 2

选项 3

排除的 **IP** 地址范围

添加 添加一个 IP 地址排除范围。最多可以添加 16 个 **US** DHCP 服务器不能分配给 DHCP 用户的排除 IP 地址范围。没有地址范围能够超过 65536 IP 地址。

起始 IP 范围 设置排除地址的起始范围。

结束 IP 范围 设置排除地址的结束范围。

删除图标　　删除排除地址范围。

6.4 查看地址租用信息

内容

进入"系统>DHCP>地址租期"，查看 DHCP 服务器分配的 IP 地址以及对应的用户 MAC 地址。

接口：全部　　刷新

IP	MAC	有效期	状态

图6.4-1　地址租期列表

接口　　选择显示租期的接口。

刷新　　点击"刷新"更新地址租期列表。

IP　分配的 IP 地址。

MAC　　被分配使用 IP 地址的设备的 MAC 地址。

有效期　DHCP 租期过期的日期与时间。

6.4.1 为具体的用户保留 IP 地址

内容

根据用户设备 MAC 地址与连接类型、常规以太网连接或 IPSec 连接；您可以为具体的用户保留一个 IP 地址。DHCP 服务器将总是将保留的地址分配给该用户。您最多可以定义 50 个保留地址。

使用 CLI 命令 system dhcp reserved-address 实现以上操作。详细信息，参见 ZXSEC US 设备 CLI 使用参考手册。

第7章 系统配置

7.1 概述

描述

本章关于 ZXSEC US 设备几项非网络性功能配置的说明，如 HA（高可用性）、SNMP、替换信息、与 VDOM 操作。

HA、SNMP 以及替换信息是 ZXSEC US 设备全局配置的一部分。更改操作模式将应用到每个 VDOM。

内容

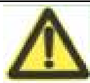
本章内容如下：

7.2 HA 高可用性

内容

ZXSEC US 设备的 HA 属性提供的增强的可靠性与性能是对网络安全级别要求较高的企业所提出的解决方案中关键的需求。以下是基于 web 管理器的（HA）高可用性配置选项、HA 虚拟群集、HA 统计表与断开群集成员连接的说明。

有关如何配置与操作 US HA 群集的详细信息，参见 ZXSEC US 设备高可用性手册以及中兴通讯网站知识库板块。

注意：

USOS v3.0 MR2 以及之前的版本中，HA 章节中包括了对 HA 属性的详细说明。从 USOS v3.0 MR3 开始，有关这部分的叙述转移到了 ZXSEC US 设备 HA 概述或 ZXSEC US 设备 HA 使用指南。

其他型号的 ZXSEC US 设备中 HA 属性均是可用的，包括 ZXSEC US70 设备。

包括以下内容：

- HA 选项
- 群集设备列表
- 查看 HA 信息
- 更改从属设备主机名称以及设备优先级别
- 从群集中断开一个群集设备的连接

7.2.1 配置 HA 选项

内容

配置 HA 选项，使 ZXSEC US 设备加入 HA 群集，或更改群集的配置或群集成员。

进入“系统>配置>HA”，配置设备的 HA 选项，以便设备可以加入一个 HA 群集。进入“系统>配置>HA”显示群集设备的名单，可以更改主设备的配置设置。在群集设备列表中，点击主设备对应的编辑图标，对配置进行更改。更改的主设备配置将同步到其他群集设备。

高可用性

模式 主动-主动

设备优先级 128

集群设置

组名 US-HA

密码

☑ 启动会话交接

	端口监控	心跳线接口	
		应用	优先级(0-512)
port1	☐	☐	0
port10	☐	☐	0
port2	☑	☑	0
port3	☐	☑	0
port4	☐	☑	0
port5	☐	☑	0
port6	☐	☐	0
port7	☐	☐	0
port8	☐	☐	0
port9	☐	☐	0

确定 取消

图7.2-1 ZXSEC US 设备的 HA 配置

注意：

如果您的 ZXSEC US 群集使用虚拟域，您可以配置 HA 虚拟群集。大多数虚拟群集 HA 选项与常规的 HA 选项相同。但是，虚拟群集包括 VDOM 分区选项。常规 HA 与虚拟群集的 HA 配置的其他不同之处参见 ZXSEC US 设备 HA 概述或 ZXSEC US 设备 HA 使用指南。

配置虚拟群集的 **HA** 选项

作为 admin 管理员登录，点击“全局配置”并进入系统管理>配置>HA，可以对 ZXSEC US 设备配置启动了虚拟域配置的 HA 选项。

作为 admin 管理员登录点击“全局配置”并进入系统管理>配置>HA 显示群集设备列表，您可以更改启动了虚拟域配置的群集中主设备的配置设置。

高可用性

模式 主动-主动

设备优先级 128

集群设置

组名 US-HA

密码

☑ 启动会话交接

	端口监控	心跳线接口	
		应用	优先级(0-512)
port1	☐	☐	0
port10	☐	☐	0
port2	☑	☑	0
port3	☐	☑	0
port4	☐	☑	0
port5	☐	☑	0
port6	☐	☐	0
port7	☐	☐	0
port8	☐	☐	0
port9	☐	☐	0

确定 取消

图7.2-2 ZXSEC US 虚拟群集配置

模式 您可以配置设备加入 HA 群集或将群集中的设备还原为单机模式。当配置一个 HA 群集时,您必须对每台设备配置相同的 HA 模式。可设置的模式包括:单机模式,主动－主动(A-A),主动－被动(A-P)。如果您配置使用虚拟群集则不可以使用主动-主动模式。

群集设备的优先级别设置 作为可选项，可以设置群集设备的优先顺序。每台群集设备都可以设置不同的优先级别。HA 通信协商中，优先级设置最高的设备便成为主设备。

虚拟群集配置中，群集设备在两个虚拟群集中都具有优先级设置值。HA 通信协商时，不管是在哪个虚拟群集，优先值设置较高的设备始终会成为主设备。

设备优先级设置不是主从设备同步属性。在一个正在运行的 HA 群集中，您可以更改群集中设备的优先级别。每当您更改一台群集设备的优先级别，群集将重新进行通信协商并且优先级别设置较高的设备成为主设备。

组名称 HA 群集的名称，名称设置的最大长度为 7 个字符。设备形成于群集之前，所有的群集设备必须具有相同的组名称。群集生效运行后，也可以更改组名称，新的组名称将同步到所有的群集设备。默认的组名称为 US-HA。您可以使用默认的组名称，也可以根据需要更改。同一网络中的两个群集不能设置相同的组名称。

群集密码设置 设置 HA 群集的密码。所设密码必须与所有群集设备的密码相同。密码的长度最多可以为 15 位的字符。默认的配置没有密码。您可以接受默认的设置或根据需要配置密码。如果同一网络中设置了不止一个 ZXSEC US 群集，每个群集必须设置不同的密码。

启动会话续接 如果群集中主设备发生故障，启动会话续接功能，全部的会话将由新的主设备续接。默认配置下没有启动会话续接功能。根据需要进行配置。

端口监控 启动或撤消对 ZXSEC US 设备接口的监控可以校验该接口是否工作正常以及是否与网络的连接通畅。

如果被监控的接口的发生故障、从网络断开或断开与群集的连接就会发生链接故障。链接故障可以使群集对该接口处理的数据包重新路由到群集中其他与网络连接的设备，其他群集设备便成为新的主设备。

默认不启动端口监控。可以保持默认设置，在群集运行后，只对连接的接口配置端口监控功能。

最多可以配置监控 16 个接口。这样的配置极限只适用于具有多于 16 个物理接口的设备。

心跳接口 启动或断开群集中每个接口的 HA 心跳通信并设置心跳接口的优先级。优先级设置最高的接口处理所有的心跳流量。如果两个或多个心跳接口具有相同的优先级设备，那么心跳接口列表中列首位的接口将处理所有的心跳流量。

对于不同型号的 ZXSEC US 设备，默认的心跳接口配置也不同，但是通常设置两个心跳接口的优先级为 50。如果默认的两个或一个心跳接口已被连接，您可以接受默认的心跳接口配置。

心跳接口的优先级设置范围是 0 到 512。新建心跳接口的默认优先级为 0。

您必须选择至少一个心跳接口。如果心跳通信被中断，群集将停止处理流量。

HA 心跳接口相互通信群集会话信息，保持同步的群集配置与群集路由表并通报各个群集设备的状态信息。HA 心跳保持 HA 状态信息的连续通信确保群集工作正常。

您也可以对物理接口设置启动心跳通信，但是对 VLAN 子接口、IPSec VPN 接口、冗余接口以及 802.3ad 集合接口不可以设置心跳通信。这些类型的接口在心跳接口列表中。

对更多的接口设置 HA 心跳可以增加网络运行的可靠性。如果一个接口失败，HA 心跳可以转移到其他接口。

VDOM 分区 您最多可以设置 8 个心跳接口。这样的限制只适用于多于 8 个接口的 ZXSEC US 设备。如果你配置虚拟群集，您可以选择在虚拟群集 1 和虚拟群集 2 中的虚拟域。Root 虚拟域必须总是在虚拟群集 1 中。

群集设备列表

进入成员列表，可以查看群集设备的操作状态，以及群集设备应用的操作模式。

进入系统管理>配置>HA，显示群集设备列表信息。



图7.2-3 ZXSEC US 设备群集列表示例

启动虚拟域配置后，您可以显示群集设备列表查看正在运行的设备状态信息。虚拟群集设备列表显示两个虚拟群集的状态信息包括添加在每个虚拟群集中的虚拟域。

作为 admin 管理员登录，点击全局配置进入系统管理>配置>HA，先是正在运行群集的虚拟群集列表。

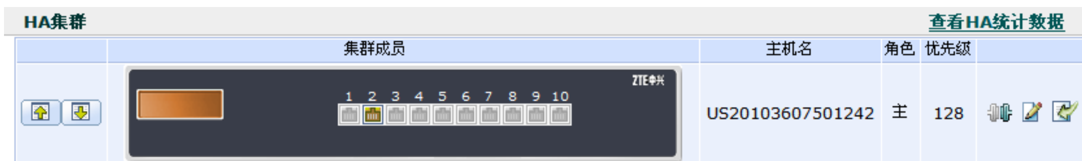


图7.2-4 ZXSEC US 虚拟群集列表示例

查看 HA 统计信息显示每台群集设备的序列号、状态、与监控信息。

向上与向下箭头 更改列表中显示的群集设备的顺序，群集中运行的设备不受影响。

群集设备群集中设备前面板的显示图。如果设备前面板上的接口显示呈现绿色状态表示接口已连接。将鼠标在前面板上停顿将显示该群集设备的主机名称、序列号、运行时间信息。设置监控的接口也将显示。

主机名称ZXSEC US 设备的主机名称。默认的 ZXSEC US 设备主机名称是设备的序列号。

进入系统管理>状态,点击当前使用主机名称旁边的“更改”可以更改主设备的主机名称。

在群集设备列表中选择一个从属设备并点击对应的编辑图表可以更改从属设备的主机名称。

角色 群集中各个设备的角色。显示“MASTER”表示该设备作为群集中的主设备。显示“SLAVE”表示作为群集中的从属设备。

优先级别 群集中设备的优先级别设置。每个设备均设置为不同的优先级别。在 HA 通信协商的过程中，级别设置较高的设备奖成为主设备。优先级别的设置范围是 0 到 255。默认的级别设置是 128。

断开与群集的连接 断开与群集的连接。参见“断开群集中的设备与群集的连接”。

编辑图标 点击编辑图标可以更改群集设备的 HA 配置。

对于群集中的主设备，点击编辑图标可以更改主设备鱼群集的 HA 配置。参见“HA 选项”。

对于一个虚拟群集中的主设备，点击编辑图标可以更改虚拟群集的 HA 配置以及虚拟群集 1 与虚拟群集 2 中设备的优先级别设置。

对于从属设备，点击编辑图标可以更改从属设备的主机名称与优先级别设置。参见“更改从属设备的主机名称与设备优先级别设置”。

对于一个虚拟群集中从属设备，点击编辑图标可以更改从属设备的主机名称。另外，您还可以更改所选的虚拟群集中从属设备设备的优先级别。如果您将该从属设备的优先级别更改为更高的设置，虚拟群集中改设备奖成为主设备。

下载调试日志　　下载加密的调试日志。您可以将该调试日志文件发送到中兴通讯技术支持中心http://support.zte.com.cn以诊断 ZXSEC US 设备的问题与故障。

查看 HA 统计表

在群集设备列表，您可以点击“查看 HA 统计数据”显示每个群集设备的序列号、状态以及监控信息。

进入系统管理>配置>HA，点击“查看 HA 统计数据”查看 HA 统计表信息。

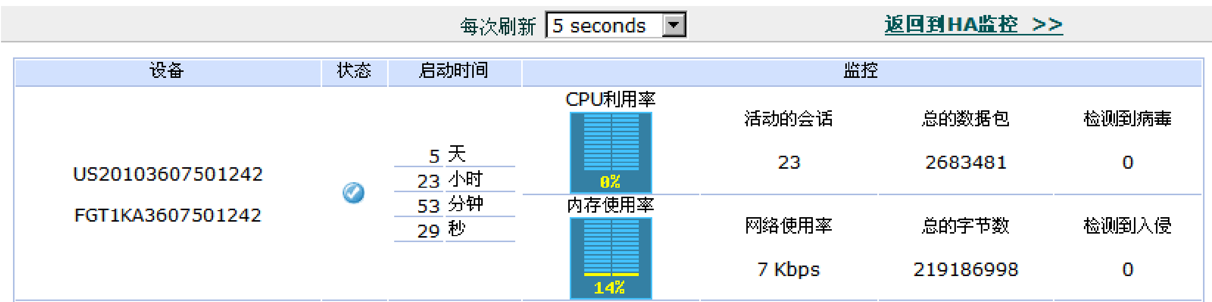


图7.2-5　**HA** 统计信息列表示例（主动-被动模式）

刷新间隔　　选择刷新间隔的时间，即基于 web 的管理器升级系统状态显示的频率。

返回到 HA 监控页面　点击“返回到 HA 监控”链接返回到群集设备列表页面。

序列号　使用序列号 ID 识别群集中每台 ZXSEC US 设备。群集 ID 与 ZXSEC US 设备的序列号相匹配。

状态信息　　显示每台群集设备的状态信息检查框呈绿色对勾表示设备正常运行。红色打叉表示设备不能与主设备建立通信连接。

运行时间　　以天、小时、分钟、秒计距离群集设备上一次启动的时间。

监控器 显示每台群集设备的系统状态信息。

CPU 占用率 每台群集设备的 CPU 使用状态信息。基于 web 的管理器只显示核心进程的 CPU 使用情况。管理进程使用 CPU 状况不显示（如，与基于 web 的管理器的 HTTPS 连接）。

内存使用率 每台群集设备的内存使用情况信息。基于 web 的管理器只显示核心进程的内存使用情况。管理进程使用内存状况不显示（如，与基于 web 的管理器的 HTTPS 连接）。

动态会话 群集设备处理的通讯会话的数量。

数据包处理 自上一次启动后群集设备处理的数据包数量。

病毒检测 群集设备检测到病毒的数量。

网络使用率 所有的群集设备接口使用过程中所占用的带宽。

字节总数 自上一次设备启动后，群集设备处理的字节数量。

入侵检测 群集设备检测到入侵与攻击的数量。

更改从属设备的主机名称与优先级别设置

在群集设备列表中，您可以更改任何从属设备的主机名称与优先级别设置。更改设备的优先级别可以导致群集重新的通信协商。

进入系统管理>配置>HA 并点击群集设备列表中从属设备对应的编辑图标可以更改从属设备的主机名称与优先级别设置。

图7.2-6 更改从属设置的主机名称与设备优先级别设置

对等设备查看或更改从属设备的主机名称。

优先级别查看或更改从属设备的优先级别设置从属设备的优先级别设置不是同步的。对于正在运行的群集，您可以更改设置的优先级别设置。群集设备优先级别设

置更改后群集将重新进行通信协商并将级别设置最高的设备更改为主设备。设备的优先级别设置范围是 0 到 255。默认的优先级别设置为 128。

断开群集设备与群集的连接

使用以下操作步骤在不中断群集操作的情况下断开某台设备与群集的连接。如果您欲将群集中的某台设备用作其他用途，如作为单机防火墙使用，您可以断开该设备与整个群集的连接。

从群集中断开群集设备的连接

1. 进入系统管理>配置>HA 查看群集设备列表。选择将要从群集中断开的设备，并点击“断开与群集连接”的图标。断开设备的连接不会中断群集的操作。

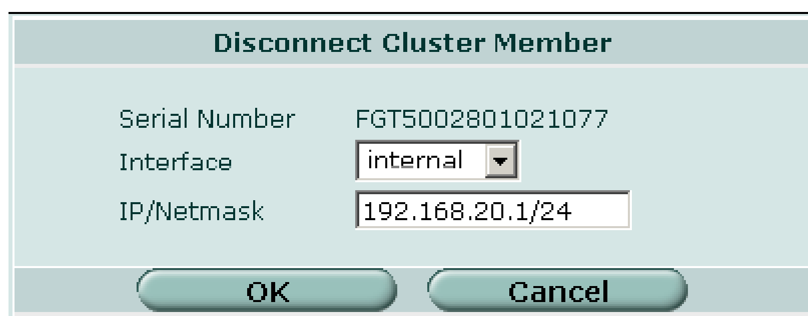


图7.2-7 断开一台群集设备与群集的连接

序列号 显示从群集中断开设备的序列号。

接口 选择要配置的接口。您可以对该接口制定 IP 地址与掩码。当设备从群集断开时，该接口的所有管理访问选项都将启动。

IP/掩码 设定接口的 IP 地址与掩码。您可以使用该 IP 地址连接该接口对已断开的设备进行配置。

2. 点击 OK 确认。

ZXSEC US 设备断开与群集的连接。群集将重新进行通讯协商并选出新的主设备。以上在图中选择的断开的设备的接口配置了制定的 IP 地址与掩码。

7.3 SNMP

配置使用 SNMP

使用简单网络管理协议（SNMP: Simple Network Management Protocol）可以监控网络中的硬件。您可以配置 ZXSEC US 设备使用 SNMP 代理用于报告系统信息并发送陷阱（警报或事件消息）到 SNMP 管理器。通过 SNMP 管理器，您可以从配置使用了 SNMP 管理访问的任何 ZXSEC US 设备接口或 VLAN 子接口访问 SNMP 陷阱与数据信息。

注意：

部分配置的 SNMP 管理器将在 ZXSEC US 设备的团体中列出的作为主机，将被监控。否则，SNMP 监控从 ZXSEC US 设备接收不到任何的陷阱，或访问陷阱。

US SNMP 执行程序是只读的。SNMP v1 与 v2c 兼容 SNMP 服务器对 ZXSEC US 系统信息具有只读的访问，并可以接收 US 陷阱。如果要监控 ZXSEC US 系统信息与接收 US 陷阱，您必须导入中兴通讯自定义的 SNMP 事件的 MIB，或中兴通讯支持的标准的 MIB。

RFC 支持包括对多数 RFC 2665 的支持（Ethernet-like MIB）与多数的 RFC 1213（MIBII）（详细信息，参见“US MIB”）。

配置使用 SNMP

进入系统管理>配置>SNMP v1/v2c，配置 SNMP 代理。

SNMP 代理　☑启用

描述

位置

联系

应用

SNMP 团体　　新建

团体名称	询问	陷阱	启用	
public	✓	✓	☑	

图7.3-1　配置使用 **SNMP**

SNMP 代理　选中功能框，启动 US SNMP 代理。

描述　　输入有关 ZXSEC US 设备的描述性信息。信息长度最多可以为 35 个字符。

位置　　输入 ZXSEC US 设备所放置的物理位置。位置描述最多可以为 35 个字符。

联系　　输入负责管理该 ZXSEC US 设备的人员联系信息。联系信息最多可以为 35 个字符。

应用　　点击“应用”，保存“描述”“位置”“联系人”信息的修改。

新建　　点击“新建”添加新的 SNMP 团体。参见 125 页“配置 SNMP 团体”。

团体名称　　添加在 ZXSEC US 配置的 SNMP 团体列表。最多可以添加 3 个团体。

名称　　SNMP 团体的名称。

询问　　每个 SNMP 团体的查询状态信息。查询状态设置可以启动或关闭。

陷阱　　每个 SNMP 团体的陷阱信息。陷阱状态设置可以启动或关闭。

启用　　选中“启用”功能框激活 SNMP 团体。

删除图标　　点击该图标删除一个 SNMP 团体。

编辑/查看图标　　查看或修改一个 SNMP 团体。

SNMP 团体

SNMP 团体就是用于网络管理的设备分组。添加 SNMP 团体使 SNMP 管理器能够连接到 ZXSEC US 设备以便查看系统信息与接收 SNMP 陷阱。最多可以添加 3 个 SNMP 团体。每个团体都针对 SNMP 查询与陷阱做了不同的配置。SNMP 团体都可以配置用来监控 ZXSEC US 设备的不同事件。每个团体最多可以添加 8 个 SNMP 管理器 IP 地址。

定义SNMP团体

组名

管理主机

IP地址	接口	删除
0.0.0.0	ANY	
	ANY	

新增

查询

协议	端口	启用
v1	161	☑
v2c	161	☑

陷阱

协议	本地	远端	启用
v1	162	162	☑
v2c	162	162	☑

图7.3-2 SNMP 团体选项（第一部分）

SNMP事件	启用
CPU过载	☑
内存太低	☑
磁盘日志空间太少	☑
HA集群状态改变	☑
HA心跳线失败	☑
HA 成员启动	☑
HA成员断开	☑
接口IP地址更改	☑
检测到病毒	☑
检测到超过大小的文件和邮件	☑
检测到文件名阻断	☑
检测到分片邮件	☑
IPS特征值	☑
IPS异常	☑
VPN隧道激活	☑
VPN隧道停止	☑

图7.3-3 SNMP 团体选项（第二部分）

组名 输入用来识别 SNMP 团体的名称。

管理主机 识别 SNMP 管理器以便使用该 SNMP 中的设置监控 ZXSEC US 设备。

IP 地址 SNMP 管理器的 IP 地址能够调用 SNMP 团体的设置监控 ZXSEC US 设备。也可以将 IP 地址设置为 0.0.0.0 以便任何 SNMP 管理器都能够使用该 SNMP 团体。

接口 作为可选设置项，可以设置该 SNMP 管理器用来连接到 ZXSEC US 设备的接口。如果 SNMP 管理器与 ZXSEC US 设备不在相同的子网，只要设置一个接口即可。如果 SNMP 管理器在互联网中或路由器之后，会发生以上所述必须设置接口的情况。

删除 点击“删除”图标删除一个 SNMP 管理器。

新增　　添加更多的 SNMP 管理器。一个 SNMP 团体中最多可以添加 8 个 SNMP 管理器。

查询　　输入端口编号（默认是 161）；该团体中 SNMP 管理器使用端口编号进行 SNMP v1 与 SNMPv2c 查询从 **ZXSEC US** 设备接收的配置信息。选中启动功能框可以激活查询功能。

陷阱　　输入本地与远程端口编号（默认是 162）；ZXSEC US 设备使用该端口发送 SNMP v1 与 SNMP v2c 陷阱到该团体的 SNMP 管理器选中“启动”功能框可以激活陷阱功能。

SNMP 事件　选中“启动”功能框便可以选择 ZXSEC US 设备应该发送给该团体中 SNMP 管理器的 SNMP 事件。“温度过高”或“电压超出范围”的事件陷阱只有在 US5001 设备中可用。

配置到接口的 SNMP 访问

一个远程 SNMP 管理器能够连接到 ZXSEC US 设备代理之前，您必须配置一个或更多的 ZXSEC US 接口接收 SNMP 连接。

1. 进入“系统>配置>接口”。
2. 选择一个 SNMP 管理器能够连接到的接口并点击“编辑”。
3. 在“管理访问”选项中，选择 SNMP。
4. 点击 OK 确认。

透明模式下配置到接口的 SNMP 访问

1. 进入系统管理>配置>接口。
2. 输入用于管理访问的 IP 地址与管理 IP/掩码字段中的掩码。
3. 点击“应用”确认。

US MIB

US SNMP 代理功能支持 ZXSEC US 公司编码的 MIB 与标准 RCF 1213 以及 RFC 2665 MIB。RFC 支持包括对应用于 ZXSEC US 设备配置的部分 RFC 2665（Ethernet-like MIB）与部分 RFC 1213（MIB II）的支持。

US MIB 以及两个 RFC MIB。您可以从中兴通讯技术支持获得这些 MIB 文件。与 SNMP 代理建立通信，您必须将这些 MIB 文件编码到 SNMP 管理器。

您的 SNMP 管理器的管理资料库中可能已经含有标准与专有的 MIB。您必须在该资料库中添加中兴通讯编制的 MIB。如果您的 SNMP 管理器中已经装有中兴通讯 SNMP 代理使用标准的 MIB，您无需重新编制该 MIB。

US MIB

MIB 文件名或 RFC　　描述

中兴通讯 MIB 是 ZXSEC US 专用的 MIB,包括详细的 ZXSEC US 系统配置信息。将该 MIB 添加到您的 SNMP 管理器可以监控所有 ZXSEC US 配置的设置以及从 SNMP 代理接收陷阱。参见“ZXSEC US 设备陷阱”与“中兴通讯 MIB 字段”。

RFC-1213(MIB II)　　US SNMP 代理支持大部分 MIB II(除了以下所列的组项):

- 不支持 EGP 组（RFC1213，3.11 与 6.10 部分）。
- 返回到 MIB II 组的协议统计表。

  （IP/ICMP/TCP/UDP 等协议）不能够准确捕获所有的 ZXSEC US 流量。更多准确的信息可以从中兴通讯 MIB 获得。

RFC-2665　　US SNMP 代理支持大部分 Ethernet-likeMIB 信息（除了以下所列的组项）。

(Ethernet-like MIB)　　不支持 dot3Test 与 dot3Error 组。

US 陷阱

ZXSEC US 代理可以将陷阱信息发送到在 SNMP 团体中添加的 SNMP 管理器。要接收陷阱，您必须将接收到的陷阱信息下载并将中兴通讯陷阱 MIB（文件名：中兴通讯.trap.3.0.mib）导入到 SNMP 管理器。

所有的陷阱包括陷阱信息以及 ZXSEC US 设备序列号与主机名称。

常规的 US 陷阱

陷阱信息	描述
ColdStart WarmStart LinkUp LinkDown	RFC1215 中所述标准的陷阱

US 系统陷阱

陷阱信息	描述
CPU 占用率过高 （fn TrapCpuHigh）	CPU 占用率超过 90%。该阀值可以使用 CLI 命令 config system global 配置。
内存过低 （fn TrapMemLow）	内存使用率超过 90%。该阀值可以使用 CLI 命令 config system global 配置。
接口 IP 更改 （fnTraplpChange）	ZXSEC US 接口的 IP 地址更改。陷阱信息包括接口名称、接口的新 IP 地址以及 ZXSEC US 设备的序列号该陷阱可以用来追踪使用 DHCP 或 PPPoE 动态分配 IP 地址后 IP 地址的变更信息。
（fnTraplfChange）	没有信息。接口更改 IP。只发送用来监控 USM 设备。
（fnTrapConfChange）	ZXSEC US 设备所做的任何配置更改信息，不包括通过与之连接的 USM 设备所做的任何配置更改。

US VPN 陷阱

陷阱信息	描述
开通 VPN 通道 (fn TramVpn TunUp)	启动 IPSec VPN 通道
关闭 VPN 通道 (fn TrapVpn TunDown)	关闭 IPSec VPN 通道

US IPS 陷阱

陷阱信息	描述
IPS 异常 fn TraplpsAnomaly	检测到 IPS 异常特征
IPS 特征 fn TraplpsSignature	检测到 IPS 特征

US 反病毒陷阱

陷阱信息	描述
检测到病毒 (fn TrapAvEvent)	ZXSEC US 检测到病毒信息并将从 HTTP 或 FTP 下载的文件或从邮件信息中删除受病毒感染的文件
检测到超大的文件/邮件 (fnTrapAvOversize)	ZXSEC US 设备检测反病毒扫描发现超大容量的文件

检测到与屏蔽文件名称相匹配的文件名 (fnTrapAvPattern)	ZXSEC US 设备检测反病毒扫描检测到与所屏蔽文件模式相匹配的文件
检测到分片邮件 (fnTrapAvPattern)	ZXSEC US 设备检测反病毒扫描检测到分片文件或附件

US 日志陷阱

陷阱信息	描述
日志已满 (fn TrapLog Full)	带有硬盘的 ZXSEC US 设备,硬盘使用空间已超过 90%。不带硬盘的 ZXSEC US 设备,日志对内存的占用已超过 90%。该阀值可以使用 CLI 命令 system global 配置。

US HA 陷阱

陷阱信息	描述
HA 切换 (fn TrapHaSwitch)	HA 群集中主设备发生故障，并有新的主设备替代
HA 心跳故障 (fnTrapHaHBFail)	HA 监控的接口发生心跳故障

USBridge 陷阱

陷阱信息	描述
USBridge 检测到故障 (fn TrapBridge)	USBridge 检测到一台 ZXSEC US 设备发生故障

MIB 字段

中兴通讯 MIB 包含能够说明当前 ZXSEC US 设备状态信息的几个字段。下表所列是 MIB 字段的名称以及对应的设备的状态信息。您可以通过将中兴通讯.3.00mib 文件导入 SNMP 管理器并浏览中兴通讯 MIB 字段查看所有字段的详细信息。

系统 MIB 字段

MIB 字段	描述
fnSysModel	ZXSEC US 设备型号。
fnSysSerial	ZXSEC US 设备序列号。
fnSysVersion	当前运行于 ZXSEC US 设备的固件版本本号信息。

MIB 字段	描述
fnSysVersionAV	安装在 ZXSEC US 设备中的反病毒定义版本号信息。
fnSysVersionNids	安装在 ZXSEC US 设备中的攻击定义版本号信息。
fnSysHaMode	ZXSEC US 高可用性（HA）模式（单机，主动-主动，主动-被动）。
fnSysOpMode	ZXSEC US 设备的操作模式（NAT 或透明模式）。
fnSysCpuUsage	当前 CPU 使用率（百分比表示）。
fnSysMemUsage	当前内存占用量（用 MB 表示）。
fnSysSesCount	当前 IP 会话数量。
fnSysDiskCapacity	硬盘容量（用 MB 表示）。
fnSysDiskUsage	当前硬盘的占用量（用 MB 表示）。
fnSysCount	当前 IP 会话计数。

HA MIB 字段

MIB 字段	描述	
fnHaSchedule	主动-主动(A-A)模式下负载平衡排程。	
fnHaStats Table	群集中每台 ZXSEC US 设备信息。	
	fnHaStatsIndex	群集中的设备索引编号。
	fnHaStatsSerial	ZXSEC US 设备序列号。
	fnHaStatsCpuUsage	当前 ZXSEC US 设备 CPU 占用率（百分比）。
	fnHaStatsMemUsage	当前 ForiGate 设备的内存使用量（MB）。
	fnHaStatsNetUsage	当前设备网络利用率（Kbps）
	fnHaStatsSesCount	ZXSEC US 设备处理的会话数量。
	fnHaStatsPktCount	ZXSEC US 设备处理的数据包数量。
	fnHaStatsByteCount	ZXSEC US 设备处理的字节数量。
	fnHaStatsIdsCount	过去 20 小时中运行于 ZXSEC US 设备的 IPS 检测到的攻击数量。
	fnHaStatsAvCount	过去 20 小时中运行于 ZXSEC US 设备反病毒系统检测到的病毒数量。

管理员帐户

MIB 字段	描述
fnAdminNumber	ZXSEC US 设备中设置的的管理员数量。
fnAdminTable	管理员列表。

	fnAdminindex	管理员帐户索引编号。
	fnAdminName	登录管理员帐户的用户名。
	fnAdminAddr	管理员使用的被信任的主机与子网的 IP 地址。
	fnAdminMask	FnAdminAddr 的掩码。

本地用户

MIB 字段	描述	
fnUserNumber	ZXSEC US 设备本地用户数量。	
fnUserTable	本地用户列表。	
	fnUserIndex	本地用户帐户索引编号。
	fnUserName	本地用户帐户的用户名列表。
	fnUserAuth	本地用户的验证类型： local-存储在 ZXSEC US 设备中的密码 radius-single—存储在 RADIUS 服务器的密码。 radius-multiple—任何通过 RADIUS 服务器验证的用户均可登录。 idap—存储在 LDAP 服务器的密码。
	fnUserState	本地用户设置是否启动或已关闭。

选项

MIB 字段	描述
fnOptIdleTimeout	设置限制超时(以分钟计);管理员必须从新接受认证。
fnOptAuthTimeout	闲置超时，用户必须接受防火墙的重新认证。
fnOptLanguage	基于 web 管理器使用的语言。
fnOptLcdProtection	设否设置了 LCDPIN。

日志

MIB 字段　描述

fnLogOption 日志参数选择。

用户定制信息

MIB 字段 描述

fnMessages ZXSEC US 设备中设置的用户信息。

虚拟域

<table>
<tr><th>MIB 字段</th><th colspan="2">描述</th></tr>
<tr><td>fnVdNumber</td><td colspan="2">ZXSEC US 设备中设置的虚拟域数量。</td></tr>
<tr><td rowspan="3">fnVdTable</td><td colspan="2">虚拟域列表。</td></tr>
<tr><td>fnVdIndex</td><td>ZXSEC US 设备设置内部虚拟域的索引数量。</td></tr>
<tr><td>FnVdName</td><td>虚拟域的名称。</td></tr>
</table>

活动 **IP** 会话

MIB 字段	描述
fnlpSessIndex	活动 IP 会话的索引编号。
fnlpSessProto	会话的 IP 协议类型（TCP,UDP,ICMP 等）。
fnlpSessFromAddr	活动 IP 会话的源 IP 地址。
fnlpSessFromPort	活动 IP 会话的源端口。
fnlpSessToPort	活动 IP 会话的目标 IP 地址。
fnlpSessToAddr	活动 IP 会话的目标端口。
fnlpSessExp	会话过期时间或会话有效期。

拨号 **VPN**

MIB 字段	描述
fnVpnDailupIndex	拨号 VPN 对等的索引。
fnVpnDailupGateway	远程网关 IP 地址。
fnVpnDailupLifetime	VPN 通道有效期
fnVpnDailupTimeout	直到下一个密钥更换时的剩余时间（以秒计）。
fnVpnDailupSrcBegin	远程子网 IP 地址。
fnVpnDailupSrcEnd	远程子网掩码。
fnVpnDailupDstAddr	本地子网 IP 地址。

VPN

MIB 字段	描述
fnVpnTunEntIndex	VPN 通道的唯一索引号。
fnVpnTunEntPhase1Name	对阶段 1 配置的描述性名称。
fnVpnTunEntPhase2Name	对阶段 2 配置的描述性名称。
fnVpnTunEntRemGwylp	远程网关的 IP 地址。
fnVpnTunEntRemGwyPort	远程网关的端口。
fnVpnTunEntLocGwylp	本地网关的 IP 地址。
fnVpnTunEntLocGwyPort	本地网关的端口。
fnVpnTunEntSelectorSrcBeginlp	源选择器的地址范围开始的地址。
fnVpnTunEntSelectorSrcEndlp	源选择器的地址范围结束的地址。
fnVpnTunEntSelectorDstBeginlp	目标选择器的地址范围开始的地址。
fnVpnTunEntSelectorDstEndlp	目标选择器的地址范围结束的地址。
fnVpnTunEntSelectorDstPort	目标选择器端口。
fnVpnTunEntSelectorProto	选择器使用的协议数量。
fnVpnTunEntSelectorLifeSecs	通道的生命周期（以秒计）。
fnVpnTunEntSelectorLifeBytes	通道的生命周期（以字节计）。
fnVpnTunEntTimeout	通道超时的时间（以秒计）。
fnVpnTunEntInOctets	通道接收的字节数辆。
fnVpnTunEntOutOctets	通道发出的字节数辆。
fnVpnTunEntStatus	通道的当前状态，启动或关闭。

7.4 替换信息

内容

进入“系统>配置>替换信息”，更改替换信息定制 ZXSEC US 设备添加到内容流，如邮件信息、网页与 FTP 会话的报警邮件及信息。

ZXSEC US 设备将替换信息添加到各种的内容流中。例如，如果在邮件信息中检测到病毒，被病毒感染的文件将从邮件中移除并以替换信息替换。web 过滤与垃圾邮件过滤中被屏蔽的页面或邮件同样以替换信息替换。

注意：

中兴通讯公司提供的声明替换信息仅作为举例使用。

替换信息列表图

名称	描述	
邮件	替换无效mail服务.	
HTTP	替换无效http服务.	
FTP	替换无效ftp服务.	
NNTP	替代不合法的NNTP服务.	
告警邮件	替换报警服务.	
垃圾邮件	替换无效SMTP服务.	
管理	管理替换信息.	
认证	替代认证页面.	
US Service Web过滤	US Service Web过滤替代信息.	
IM和P2P	替代阻断的IM和P2P.	
SSL VPN	替代SSL VPN信息.	

图7.4-1 替换信息列表图

名称 替换信息的类型。点击蓝色三角标志可以将扩展或收缩类型显示。您可以更改以下替换信息：

- 病毒感染附件的邮件
- 网页(Http)
- FTP
- 报警邮件
- Spam
- US Service web 过滤
- IM 与 P2P

您也可以修改以下信息：

- 用户认证的登录页面
- 用户验证声明页面（一些型号的设备）
- 验证存活的页面
- US Service web 过滤屏蔽跳过页面
- SSL-VPN 的登录页面
- 相关页面的主机查看信息（只适用于 US224 设备）

描述 替换信息类型的描述基于web的管理器对于替换信息的生成的位置的描述。

编辑/查看图标　　点击该图标对替换信息进行更改。

注意：

在防火墙策略生效之前，USOS 使用 HTTP 对用户发送“验证声明”页面。因此，用户必须首先发起一个 HTTP 流量以触发验证声明页面。用户接受声明后，便可以发送防火墙策略允许的任何流量了。

7.4.1 更改替换信息

内容

消息设置：HTTP 病毒消息

允许格式： HTML

大小： 8192 (字符)

```
<HTML><BODY><h2>High security alert!!!
</h2><p>You are not permitted to download the
file "%%FILE%%" because it is infected with the
virus "%%VIRUS%%". </p><p>URL = http://%%URL%%
</p><p>File quarantined as: %%QUARFILENAME%
%.</p></BODY></HTML>
```

确定　　取消

图7.4-2　**HTTP** 病毒替换信息示例

替换信息可以是以文本或 HTML 信息格式显示。您可以将 HTML 代码添加到 HTML 信息。另外，替换信息可以含有替换信息标签。用户接收到替换信息，有关的信息内容将替换信息标签。每条替换信息最多可以是 8192 个字符组成。

另外，替换信息可以包括替换信息标签。当用户接收到替换信息时，替换信息标签将以信息相关的内容替代。表 28 所列是您可以添加的替换信息。

替换信息标签

标签	描述
%%AUTH_LOGOUT%%	URL 将立即删除当前策略并关闭会话。用于验证-保持存活页面。

标签	描述
%%AUTH_REDIR_URL%%	验证-保持存活页面将用户重新定向到链接到该标签的新窗口。
%%CATEGORY%%	网址内容类型的名称。
%%DEST_IP%%	病毒发送目的地的 IP 地址。对于邮件来说，是发送包含病毒的邮件服务器 IP 地址.对于 HTTP 而言，是发送病毒的网页的 IP 地址。
%%EMAIL_FROM%%	消息发送人的邮件地址。
%%EMAIL_TO%%	消息接收人的的邮件地址。
%%FAILED_MESSAGE%%	登录失败的信息显示在验证-登录-失败页面。
%%FILE%%	从内容流中移除文件的文件名该文件可以为含有病毒的文件或是被反病毒文件系统隔离的文件。 %%FILE%%可以用在病毒于文件屏蔽信息中。
%%US SERVICE_WF%%	US Service-网页过滤服务标识。
%%中兴通讯%%	中兴通讯公司的标识。
%%HC_ACTIVEX%%	ZXSEC US350A 主机查看功能的控件。
%%HC_FC_LINK%%	US350A 设备中链接到 US Desktop 主机安全软件下载界面。
%%HC_REMEDY_LINK%%	在 ZXSEC US350A 设备中链接到重新运行主机查看操作。
%%HC_URL_LINK%%	在 ZXSEC US350A 设备中链接到第三方安全软件。该链接可以在“交换>端口隔离>动态策略”中定义。
%%HTTP_ERR_CODE%%	HTTP 错误代码，例如“404”。
%%HTTP_ERR_DESC%%	HTTP 错误描述。
%%KEEPALIVEURLC%%	验证-存活-页面自动连接到该 URL，在每隔%%TIMEOUT%%的时间内更新连接策略。
%%NIDSEVENT%%	IPS 攻击信息。%%NIDSEVENT%%将被添加到报警入侵信息中。
%%OVERRIDE%%	链接到 US Service 网页过滤代理服务器的信息框。该信息只有属于被允许创建 US Service 网页过滤代理的组群的用户可以看到。
%%OVRD_FROM%%	US Service 网页过滤屏蔽代理服务器信息框。该标签必须在 US Service 网页过滤代理信息框中显示，而且不应该用在其它替换信息中。
%%PROTOCOL%%	检测到的病毒使用的传输协议。 %%PROTOCOL%%可以添加到警报邮件的病毒信息中。

标签	描述
%%QUARFILENAME%%	从内容流中移除并添加到隔离区的文件的文件名。该文件可以是包含病毒的文件或是被反病毒文件系统隔离的文件。%%QUARFILENAME%%可以用在病毒与文件屏蔽的信息中。只有当 US 设备配有本地磁盘的时候，隔离区才可用。
%%QUEATION%%	验证确认页面所要求输入的验证确认信息弹出对话框输入用户名与密码。
%%SERVICE%%	网页过滤服务的名称。
%%SOURCE_IP%%	接受到屏蔽文件的请求发送者的 IP 地址对于电子邮件来说,该 IP 地址是用户计算机试图从被删除的文件下载信息的 IP 地址。
%%TIMEOUT%%	验证存活连接之间配置的秒数，用于验证-存活页面。
%%URL%%	网页的 URL。该文件可以是网页内容过滤或 URL 屏蔽功能阻止的网页。%%URL%%也可以用在用户试图从被屏蔽的 URL 网页中下载文件的 http 病毒与文件隔离信息中。
%%VIRUS%%	反病毒系统检测到的病毒的名称。%%VIRUS%% 可以用在病毒信息中。

7.4.2 更改认证登录页面

内容

用户使 VP 或防火墙策略是需要被验证，相应弹出认证登录页面。您可以按照修改其他替换信息一样定义该页面，但是需要注意一些特别的需求：

- 登录页面必须是 HTML 格式页面，包含具有 ACTION="/" 与 METHOD="POST"的表单。
- 表单必须包含以下隐藏的控件：

  <INPUT TYPE="hidden" NAME="%%MAGICID%%" VALUE="%%MAGICVAL%%">

  <INPUT TYPE="hidden" NAME="%%STATEID%%" VALUE="%%STATEVAL%%">

  <INPUT TYPE="hidden" NAME="%%REDIRID%%" VALUE="%%PROTURI%%">

- 表单必须包含以下可见的控件：

  <INPUT TYPE="text" NAME="%%USERNAMEID%%" size=25>

```
<INPUT TYPE="password" NAME="%%PASSWORDID%%" size=25>
```

举例所示：以下是符合以上所述要求的简单的认证页面的举例：

```
<HTML><HEAD><TITLE>Firewall Authentication</TITLE></HEAD>
<BODY><H4>You must authenticate to use this service.</H4>
<FORM ACTION="/" method="post">
<INPUT NAME="%%MAGICID%%" VALUE="%%MAGICVAL%%" TYPE="hidden">
<TABLE ALIGN="center" BGCOLOR="#00cccc" BORDER="0" CELLPADDING="15" CELLSPACING="0" WIDTH="320"><TBODY>
<TR><TH>Username:</TH>
<TD><INPUT NAME="%%USERNAMEID%%" SIZE="25" TYPE="text">
</TD></TR>
<TR><TH>Password:</TH>
<TD><INPUT NAME="%%PASSWORDID%%" SIZE="25" TYPE="password">
</TD></TR>
<TR><TD COLSPAN="2" ALIGN="center" BGCOLOR="#00cccc">
<INPUT NAME="%%STATEID%%" VALUE="%%STATEVAL%%" TYPE="hidden">
<INPUT NAME="%%REDIRID%%" VALUE="%%PROTURI%%" TYPE="hidden">
<INPUT VALUE="Continue" TYPE="submit"> </TD></TR>
</TBODY></TABLE></FORM></BODY></HTML>
```

更改 **US Service** 网页过滤屏蔽跳过页面

%%OVRD_FROM%%标签提供如果 US Service 网页过滤服务屏蔽对一个网页访问时用于发起一个代理的表单。请不要从替换信息中删除该标签。

更改 **SSL-VPN** 登录信息

SSL VPN 登录信息是一个 web 页面，通过该页面用户可以登录到 SSL-VPN 门户。该门户网站可以链接到ZXSEC US 设备的一些功能项您必须根据以下指导进行构建，以便这些功能能够运行正常。

- 登录页面必须是包含 ACTION="%%SSL_ACT%%" 与 METHOD="%%SSL_METHOD%%"表单的 HTML 页面。
- 必须包含%%SSL_LOGIN%%标签的表单，用于提供登录表单。
- 表单必须包含%%SSL_HIDDEN%%标签。

更改认证声明页面

认证声明页面是应用在一些型号的 ZXSEC US 设备，有关在 ZXSEC US 设备允许访问之前有关使用规则的声明性信息，用户必须同意该认证声明。您可以在防火墙策略中启动该认证声明。参见“防火墙策略选项”中用户认证声明信息说明。您只可以更改该声明的文本格式，而不是 HTML 表单代码。

更改主机查看页面（只适用于 **ZXSEC US350A** 设备）

扫描访问、诊救失败、隔离、允许访问与拒绝访问页面都是 HTML 格式的文本信息。您可以根据需要修改这些信息。没有特殊要求。入口页面与提交结果页面中包含特殊的选项，您不能删除。

入口页面

入口页面的显示提供下载 US Desktop 或第三方反病毒软件以诊救主机查看失败。

共两个标签链接到下载软件：

- %%HC_FC_LINK%%标签链接到 US Desktop 下载
- %%HC_URL_LINK%%链接到第三方软件下载

根据您的网络配置需要，您可以省略这些标签中的一个。例如，您只提供下载 US Desktop 软件，您便可以省略第三方软件下载的标签。

%%HC_REMEDY_LINK%%标签是必需的，因为用户可以选择在安全反病毒软件后运行主机查看程序。

提交结果页面

提交结果页面运行主机查看程序并可以提供将结果提交到 ZXSEC US350A 设备。该页面中多数选项都是必需的：

- 页面的主体标签必须含有 onload="host_checker()，那么主机查看程序才可

以执行。

- 标签%%HC_ACTIVEX%%必须显示在 HTML 页面的报头部分，以下载所需的主机查看 Activex 控件。
- 以下格式必须出现在 HTML 页面的正文中：

```
<form method=post name=recover action="%%HC_PORTAL_PAGE%%">
<input type=hidden name="%%HC_PORT_NAME%%"
value="%%HC_FROM_PORT%%">
<input type=hidden name="%%HC_TYPE_NAME%%">
<input type=hidden name="%%HC_RESULT_NAME%%">
<input class=button type=submit name="%%HC_SUBMIT_NAME%%"
value="Submit">
</form>
```

7.5 VDOM 操作模式与管理访问

内容

每个 VDOM 允许独立的进行操作模式的更改。也就是说，ZXSEC US 设备中设置的不同 VDOM 可以应用不同的操作模式。

到 VDOM 的管理访问可以根据连接 ZXSEC US 设备的接口与使用的协议来限制。

更改操作模式

您可以设置虚拟域的操作模式并执行相应得网络配置确保在新的模式下能够连接到基于 web 的管理器。

注意：

应用于交换模式下的 ZXSEC US350A 设备不支持透明模式。

7.5.1 从 NAT/路由模式切换到透明模式

内容

1. 进入“系统>配置>操作模式”或点击虚拟域状态系统状态页面中操作模式对应的更改。
2. 从操作模式列表中点击“透明模式”。

模式

工作模式 透明
管理IP/掩码 10.16.13.53/255.255.255.0
缺省网关 10.16.13.3
应用

3. 输入以下信息并点击“应用”。

管理 IP/掩码 输入管理 IP 地址与掩码该地址必须对于您管理 ZXSEC US 设备的网络来说是有效的 IP 地址。

缺省网关 输入 ZXSEC US 设备访问其他网络所需的默认的网关。

7.5.2 从透明模式切换到 NAT/路由模式

内容

1. 进入“系统>配置>操作模式”或点击虚拟域状态系统状态页面中操作模式对应的更改。
2. 从操作模式列表中点击“NAT 模式”。

模式

工作模式 NAT
应用

3. 输入以下信息并点击“应用”。

管理 IP/掩码 输入管理 IP 地址与掩码该地址必须对于您管理 ZXSEC US 设备的网络来说是有效的 IP 地址。

设备 选择接口 IP 地址/掩码应用的接口。

默认网关 输入 ZXSEC US 设备访问其他网络所需的默认的网关。

网关设备 点击选择默认的网关连接的接口。

7.5.3 管理访问

内容

您可以 VDOM 中的任何借口配置管理访问。参见“控制接口的管理访问”。NAT/路由模式下，接口的 IP 地址用于管理访问。透明模式下，您只需要配置一个管理 IP 地址并可以适用于 VDOM 中所有的接口。ZXSEC US 设备也使用该 IP 地址连接 US SERVICE 中心下载反病毒与攻击定义更新。（参见“US Service 服务订制中心”）。

普通管理员帐户只能访问该帐户属于的 VDOM。管理计算机必须与该 VDOM 中的一个接口相连接Admin 管理员能够访问所有的 VDOM以上所述两种情况下，管理计算机必须与一个允许管理访问的接口连接,并且计算机的 IP 地址与该接口的 IP 地址必须处于同一个子网中。

您可以允许对 ZXSEC US 设备的远程管理。但是，允许从互联网对 ZXSEC US 的远程管理访问可能会降低设备使用的安全性。除非配置需要，否则避免这样的远程访问操作。为了提高 ZXSEC US 设备使用的安全性，您可以使用以下连接从互联网中访问 ZXSEC US 设备：

- 使用安全管理访问设置用户及密码
- 定期更改密码
- 启动对该接口的安全管理访问，只使用 HTTPS 或 SSH。
- 尽量不要更改系统默认的闲置时间。（默认闲置时间为 5 分钟参见“设置”。）

第8章 系统管理员设置

8.1 概述

描述

本章是有关如何在 ZXSEC US 设备中设置管理员帐户的信息。管理员可以访问ZXSEC US 设备并配置其操作。在设备初始安装完成后，默认的配置只有一个用户名为 admin 的管理员帐户。通过连接到基于 web 的管理器或 CLI，您也可以配置更多的管理员具有不同级别的到不同部分的 ZXSEC US 设备的配置的管理访问。

注意：管理员结束与 ZXSEC US 的通信会话时需要在基于 web 的管理器或 CLI中退出登录。否则，会话保持打开状态。

每个管理员都有一定的访问权限级别,访问权限设置将访问 ZXSEC US 设备划分为不同的访问控制类型，这些类型决定了对 ZXSEC US 设备的读或写的权限。

内容

8.2 系统管理员

可以设置两种类型的管理员帐户：

- 普通管理员；除超级管理员之外的配置了任何管理权限的管理员。
- 系统管理员；包括默认的管理员帐户 admin，以及任何其他分配了超级管理员权限的管理员。

普通管理员帐户根据其访问权限内容访问配置选项。如果启动了虚拟域，分配到一个 VDOM 的普通管理员帐户不能访问全局配置选项以及其他任何 VDOM 的配置。有关哪些选项是属于全局配置哪些属于每个 VDOM 的详细信息，参见“虚拟域配置设置”与“全局配置设置”。

默认的管理员帐户 admin 对全部的 ZXSEC US 设备享有配置权限，另外，通过 admin 帐户还可以：

- 启动 VDOM 配置
- 创建 VDOM
- 配置 VDOM
- 给 VDOM 配置普通管理员
- 配置全局配置选项

超级管理员的访问权限不能被更改，且不出现在“系统>管理权限”的内容列表中，但是它作为系统>Admin 页面中新建/编辑管理员对话框中的访问权限下拉列表中选项之一。

新增普通管理员
普通管理员
类型 规则 远端 PKI
输入密码
密码确认
可信主机 #1 0.0.0.0/0.0.0.0
可信主机 #2 0.0.0.0/0.0.0.0
可信主机 #3 0.0.0.0/0.0.0.0
访问表 [请选择]
[请选择]
[创建新...]
super_admin
取消

图8.2-1 管理员对话框中的超级管理员选项

被分配应用超级管理员权限帐户的用户：

- 不能删除同样具有超级管理员权限的登录用户。
- 在同样具有超级管理员权限的用户没有登录的情况下，超级管理员用户可以删除这些用户，以及更改配置的验证方式、密码、管理权限。
- 只有在其他同样具有超级管理员权限的用户登录后，且默认的 admin 没有登录的情况下，可以删除默认的 admin 帐户。

注意：具有超级管理员权限的用户，可以使用 CLI 重新设置密码。如果您更改了一个已登录用户的密码，那么该用户将退出登录，使用新的密码重新被验证后登录。

将具有超级管理员权限的用户 ITAdmin，将密码更改为 123456：

```
config sys admin
edit ITAdmin
set password 123456
end
```

将具有超级管理员权限的用户 ITAdmin，将密码从 123456 重新设定为默认的密码为空状态：

```
config sys admin
edit ITAdmin
unset password 123456
end
```

您可以使用存储在 ZXSEC US 设备或 RADIUS 服务器的密码验证管理员帐户。作为可选项，您可以将所有的管理员帐户除了 admin 帐户存储在一个 RADIUS 服务器上。相同 RADIUS 服务器上基于 RADIUS 的帐户享有相同的访问权限。

对管理员帐户配置 RADIUS 验证

如果您想使用 RADIUS 服务器验证属于您的 VDOM 的管理员帐户,在创建管理员帐户之前您必须配置验证设置。进行以上操作之前，您需要：

- 配置 ZXSEC US 设备访问 RADIUS 服务器
- 创建一个用户组，并设置 RADIUS 服务器作为其唯一的成员

以下步骤进行的前提是假设您的网络中有RADIUS服务器并且沿用您的管理员的名称与密码。有关如何建立 RADIUS 服务器的信息，参见您的 RADIUS 使用管理手册。

配置 ZXSEC US 设备访问 RADIUS 服务器

1. 进入用户>RADIUS。
2. 点击“新建”。

3.　输入以下信息：

参数名称	参数说明
名称	RADIUS 服务器的名称。在您创建用户组时可以使用该名称。
服务器名称/IP	RADIUS 服务器的域名与 IP 地址。
服务器密钥	RADIUS 服务器密钥。RADIUS 服务器管理员可以提供该信息。

4.　点击 OK 确认。

创建管理员用户组

1.　进入用户>用户组。

2.　点击“新建”。

3.　在“组名称”字段，输入管理员组的名称。

4.　从“可用用户列表”中选择 RADIUS 服务器名称。

5.　点击绿色箭头将选中名称放入“成员列表”。

6.　设置保护内容表。

7.　点击 OK 确认。

对管理员配置 PKI 证书验证

公共密钥基础设施(PKI:Public Key Infrastruture)验证利用由“对等”，“对等”组，和或用户组组成列表的证书验证库进行验证，并返回验证结果“成功”或“拒绝”的通告。用户只需要一个有效的证书便可以成功进行验证，不需要输入用户名或密码。

如果您对管理员设置使用 PKI 验证，在创建管理员帐户之前必须配置验证方式。执行以上操作，您需要：

⌘　创建一个 PKI 用户组以下步骤是在假设您的网络中应用了 RADIUS 服务器，且服务器上配置了系统管理员的名称与密码。有关怎样建立 RADIUS 服务器的信息，参见有关 RADIUS 服务器操作说明。

进入“用户>PKI”配置 PKI 用户。

PKI

名称	标题	CA

图8.2-2　用户>PKI 用户列表

参数名称	参数说明
新建	添加新建 PKI 用户。
用户名	PKI 用户名称。
主题	验证用户的证书的主题字段中显示文本字符串。
发行方	用于验证用户的 CA 证书。
删除图标	删除 PKI 用户。
编辑图标	编辑 PKI 用户。

注意：以下字段是 PKI 用户列表中对应 PKI 用户对话框中的著名字段：

用户名称：名称

主题：主题

CA：发行方（CA 证书）

配置 ZXSEC US 设备访问 RADIUS 服务器

1. 进入“用户>RADIUS”。

2. 点击“新建”。

3. 输入以下信息：

名称	RADIUS 服务器名称。在您创建用户组时使用该名称。
服务器名称/IP	RADIUS 服务器的域名或 IP 地址
服务器密钥	RADIUS 服务器密钥。RADIUS 服务器管理员可以提供该信息。

4. 点击 OK 确认。

创建管理员用户组

1. 进入“用户>用户组”。

2. 点击“新建”。

3. 在“用户名称”字段，输入管理用户组的名称。

4. 在“可用用户列表”中，选择 RADIUS 服务器名称。

5. 点击绿色向右箭头将名称移动到成员列表。

6. 设置内容保护列表。

7. 点击 OK 确认。

查看管理员列表

使用 admin 帐户或享有队新的管理员帐户具有读写权限并可以控制其允许访问级别的 admin 用户。进入系统管理>管理员设置>管理员。

除非您是 admin 管理员，管理员列表只现实当前虚拟域的管理员信息。

管理员　访问内容表　集中管理　设置

新建

管理员	可信主机	访问控制表	类型
lilj	0.0.0.0/0, 0.0.0.0/0, 0.0.0.0/0	prouser	本地
pengxl	0.0.0.0/0, 0.0.0.0/0, 0.0.0.0/0	prouser	本地
user	0.0.0.0/0, 0.0.0.0/0, 0.0.0.0/0	user	本地

图8.2-3　管理员列表

参数名称	参数说明
新建	添加管理员帐户。
管理员	登录管理员帐户的名称。
可信主机	管理员登录使用的被信息主机的 IP 地址。详细信息，参见“使用信任主机”。
访问控制表	管理员的访问权限内容默认的 admin 帐户是没有权限内容的。
类型	该管理员的验证类型： 本地-本地密码。 RADIUSRADIUS 服务器中具体帐户的验证。 RADIUS+通配符-RADIUS 服务器上对人和帐户的验证。 PKI；基于 PKI 的证书验证。
删除图标	删除管理员帐户。您不能够删除默认的 admin 管理员帐户，除非您创建了具有超级管理员权限的另外的用户。
编辑或查看图标	编辑或查看管理员帐户。
更改密码图标	更改管理员帐户的密码。

更改管理员帐户登录密码

1. 进入“系统>管理员设置>管理员”。
2. 选择所要更改密码的帐户，并点击该帐户旁边的更改密码图标。
3. 输入并确认新的密码。
4. 点击 OK 确认。

配置管理员帐户

使用 admin 帐户或具有读写权限的帐户创建一个新的管理员。进入系统管理>管理员设置>管理员并点击“新建”。

编辑普通管理员	
普通管理员	lilj
类型	◉规则 ○远端 ○PKI
可信主机 #1	0.0.0.0/0.0.0.0
可信主机 #2	0.0.0.0/0.0.0.0
可信主机 #3	0.0.0.0/0.0.0.0
访问表	prouser
返回	

图8.2-4 管理员帐户配置-**RADIUS** 验证

新增普通管理员	
普通管理员	
类型	◉规则 ○远端 ○PKI
输入密码	
密码确认	
可信主机 #1	0.0.0.0/0.0.0.0
可信主机 #2	0.0.0.0/0.0.0.0
可信主机 #3	0.0.0.0/0.0.0.0
访问表	[请选择]
OK	取消

图8.2-5 管理员帐户配置—**PKI** 验证

参数名称	参数说明
管理员	输入登录管理员帐户的名称。管理员的名称设置不能包含字符<>,(), #, " ' 。在管理员的名称设置中使用这些字符可以导致 XSS（跨站脚本）漏洞。
类型	该管理员的验证类型： ⌘ 常规：点击创建本地管理员帐户。 ⌘ RADIUS：设置使用 RADIUS 服务器验证管理员。首先必须对管理员配置 RADIUS 验证。 ⌘ PKI：设置对管理员启动基于证书的验证。只有配置的管理员每次都可以使用启动的 PKI 选项设置。

用户组	如果您使用 RADIUS 或基于证书的 PKI 验证，选择含有 RADIUS 服务器 /PKI（对等）用户作为成员的管理员用户组。一旦管理员用户组被选择用于验证将不能被删除。
通配符	选中该功能框。允许 RADIUS 服务器中所有的帐户都作为管理员。只有启动 RADIUS 功能时，该功能才可用。
密码	输入登录密码。为了增强网络使用的安全性，密码至少设置为 6 个字符长度。如果启动了 RADIUS，ZXSEC US 设备首先进行 RADIUS 验证，如果验证失败，将接着进行密码验证。以上操作均在启动了“通配符”选项后可用。
确认密码	再输入一次登录密码，确认所输密码的正确性。如果没启动“通配符”该选项不可用，以及在应用 PKI 验证情况下也不可用。
可信主机＃**1**，＃**2**，＃**3**	输入管理员登录 ZXSEC US 设备使用的主机的 IP 地址与掩码。您可以指定三个访问主机的 IP 与掩码。将所有的管理员设置可信主机 IP 与掩码可以增强网络的安全性。详细信息参见“可信主机的使用”。
访问表	管理员的访问权限预先配置的 prof_admin 权限中提供了 ZXSEC US 设备的全权访问配置。您也可以点击“新建”创建新的访问权限内容。有关访问权限的内容，参见“配置访问权限内容”。

配置管理员帐户

1. 进入“系统>管理员设置>管理员”。

2. 点击“新建”添加管理员帐户并点击编辑图标对现有的管理帐户进行编辑。

3. 在管理员字段，输入管理员帐户的登录名称。如果配置该管理员使用 RADIUS 验证，但是没有使用通配符选项，管理员名称必须与 RADIUS 服务器中的帐户相匹配。

4. 设置验证类型：对该管理员使用

RADIUS 验证，您需要：

- 选中“RADIUS”。
- 如果您想设置 RADIUS 中所有的帐户都作为该 ZXSEC US 设备的管理员帐户。
- 从用户组列表中选择管理员用户组。

设置使用基于证书的 PKI 验证管理员时：

- 选中“PKI”。
- 从管理员帐户中选择管理员用户组。

5. 输入并确认管理员帐户密码。如果您使用 RADIUS 通配符或 PKI 证书验证，并不会出现该步骤。

6. 作为可选项，输入信任主机的 IP 地址与掩码，该可信主机也就是管理员用来登录基于 web 的管理器的。

7. 设置管理员的访问权限。

8. 点击 OK 确认。

可信主机的使用对所有的管理员帐户设置可信主机，通过限制管理访问进一步增强了网络使用的安全性。管理员登录 ZXSEC US 设备时，除了需要密码外，还必须使用并通过指定的子网。如果您只定义了一个可信的主机的 IP 地址以及掩码为 255.255.255.255，那么该管理员只能通过该 IP 访问 ZXSEC US 设备。

当您对所有的管理员设置可信主机时，确保了高度的安全性，其它任何主机对 ZXSEC US 设备进行管理访问都不会得到回应如果您对其中一个管理员没有进行可以主机的设置，ZXSEC US 设备接受从启动了管理访问设置的接口进入的管理访问，潜在的将 ZXSEC US 设备暴露给未经授权的访问。

通过 telnet 或是 SSH 访问时，同样可以对基于 web 的管理器与 CLI 的访问设置可信主机。通过 console 连接器对 CLI 的访问不受影响。

可信主机的地址默认分别为 0.0.0.0./0.0.0.0，与 127.0.0.1/32。如果您设置 0.0.0.0./0.的地址为不含有零的地址，那么您可以忽略对另一个地址的设置。这是唯一使用通配符条目设置可信主机的地址。但是，改配置并不安全。

8.3 访问内容表

每个管理员帐户都设置有一定访问权限。访问权限设置将 ZXSEC US 设备的一些功能划分为不同的访问控制类型，对不同的访问控制类型您可以具有读或写的权限。下表所列是基于 web 管理器的页面中每个访问控制类型提供的访问：

基于 web 的管理器页面的访问控制设置

访问控制	相关选项设置
Admin 用户	系统>管理员设置 系统>Admin>USM 系统>Admin>设置
反病毒配置	反病毒

用户验证	用户
防火墙配置	防火墙
US Service 更新	系统>维护>US Service 中心
IPS 配置	入侵防护
日志与报告	日志与报告
维护	系统>维护
系统配置	系统>网络>接口 系统>网络>区域 系统>DHCP
路由器配置	路由器
垃圾邮件过滤配置	反垃圾邮件
系统配置	系统>状态，包括会话信息 系统>配置 系统>主机名称 系统>网络>选项 系统>Admin>USM 系统>Admin>设置 系统>状态>系统时间
VPN 配置	VPN
Web 过滤配置	Web 过滤

读的权限是指管理员能够查看基于 web 的管理器的页面中的功能选项。管理员只有具备写的权限才可以更改页面中的设置。

您可以扩展防火墙配置访问控制以实现更多的对防火墙功能的细化控制。您可以对管理员配置到策略、地址、服务、时间表、保护内容标以及其他（VIP）配置的访问。

注意：虚拟域配置启动后，具有超级管理员权限的管理员才能对全局设置进行访问配置。即使启动了虚拟域配置，普通的 VDOM 管理员也只能访问特定的虚拟域。有关哪些设置属于全局配置，参见“虚拟域配置设置”。

访问权限设置在 CLI 命令中同样对管理员访问生效。下表所示在每项访问控制类型中可以的 CLI 命令。具有读的权限可以访问“get”“show”这样的命令，访问 config 命令需要具有写的权限。

访问控制	可用的命令
Admin 用户(admingrp)	system admin system accprofile
反病毒配置(avgrp)	antivirus
用户验证(authgrp)	user
火墙配置(fwgrp)	firewall 使用 set fwgrp custom 与 config fwgrp-permission 命令单个设置一些防火墙访问许可。这些选项包括策略、地址、服务、时间表、内容保护列表以及其他(VIP)配置。
USProtect 更新(updategrp)	system autoupdate execute update-av execute update-ips execute update-now
IPS 配置(ipsgrp)	ips
日志与报告(loggrp)	alertermail log system USLA execute log
维护(mntgrp)	execute formatlogdisk execute restore execute backup execute batch execute usb-disk
网络配置(netgrp)	system arp-table system dhcp system interface system zone execute dhcp lease-clear execute dhcp lease-list execute clear system arp table execute interface

路由配置(routegrp)	router execute router execute mrouter
反垃圾邮件过滤(spamgrp)	spamfilter
系统配置(sysgrp)	system 除了 accprofile, admin, arp-table, autoupdate, USLA, interface, 与 zone. execute date execute ha execute ping execute ping-options execute ping6 execute time execute traceroute execute cfg execute factoryreset execute reboot execute shutdown execute deploy execute set-next-reboot execute ssh execute telnet execute disconnect-admin-session execute usb
VPN 配置(vpngrp)	vpn execute vpn
Web 过滤配置	webfilter

进入“管理 >管理员设置>访问权限内容表”，设置 ZXSEC US 管理员的权限。您可以创建对 ZXSEC US 设备的访问权限为拒绝访问，只读或读写权限。

如果管理员对某项功能设置只具有读的权限，也就是说管理员可以通过基于 web 的管理器页面查看该项功能,但不能对该设置进行修改。在该项设置显示的 web 管理器页面中没有“创建”或“应用”按键而且只有查看图标()而没有编辑或删除等其它修改性命令。

查看访问控制列表

进入“系统>admin>访问控制列表”。使用 admin 帐户或具有读写权限的用户帐户可以创建或编辑访问控制列表。



图8.3-1　访问内容列表

参数名称	参数说明
新建	添加新的访问权限。
内容表名称	访问权限的名称。
删除图标	点击该图标删除一项访问权限。 管理员设置的访问权限不能删除。
编辑图标	点击该图标修改访问权限。

访问权限内容表选项

进入系统管理>管理员设置>访问内容表。新建帐户并配置管理权限。

新建授权表

授权表名称:

访问控制	无	读	写
维护	◉	○	○
管理用户	◉	○	○
US Service升级	◉	○	○
授权用户	◉	○	○
系统配置	◉	○	○
网络配置	◉	○	○
Web过滤配置	◉	○	○
垃圾邮件过滤配置	◉	○	○
防病毒配置	◉	○	○
IPS配置	◉	○	○
路由配置	◉	○	○
VPN配置	◉	○	○
IM, P2P & VoIP配置	◉	○	○
防火墙配置	◉	○	○
日志与报告	◉	○	○

OK 取消

图8.3-2 访问权限选项

参数名称	参数说明
新建授权表	输入访问权限的名称。
访问控制	访问控制列表列出可以设置的访问权限的功能选项。
None	点击“none”撤消到所有访问控制种类的访问。
读	选中该功能框，允许管理员对访问控制所列的功能设置选项具有读的权限。
写	选中该功能框，允许管理员对访问控制所列的功能设置选项具有写的权限。
访问控制种类	根据需要对访问控制类型设置读写权限。有关访问控制类型的详细信息，参见“访问权限设置”。

8.4 集中管理

进入系统管理>管理员设置>集中管理，配置 **ZXSEC US** 设备接受以下服务与设备的管理：

- USM
- US Service Management Service

对于 USM 设备与 US Service 服务来讲，管理的功能性是相似的，也就是说 ZXSEC US 设备被 USM 设备与 US Service 服务集中管理。该选项允许您将 ZXSEC US 设备的配置备份到除了本地 PC 之外的其他地址，这样配置选项在您管理多个 ZXSEC US 设备时比较有用。

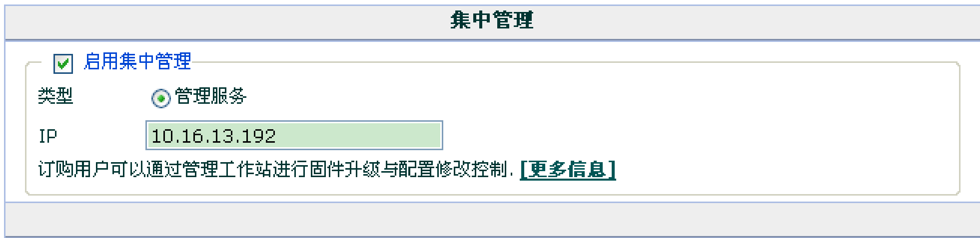
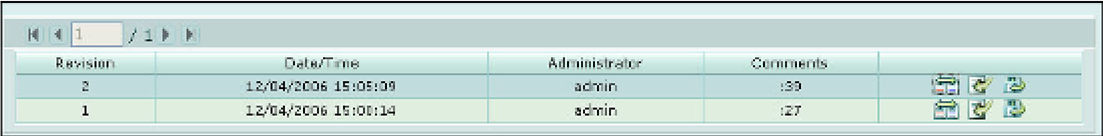


图8.4-1 集中管理配置—USM 与 US Service

配置更改控制（通过 USM 服务器或 US Service 管理服务进行管理）允许您管理多个版本的 ZXSEC US 设备配置文件。该功能需要配置集中管理服务器。ZXSEC US 设备中启动更改控制时，您便可以查看被保存的您的 ZXSEC US 设备的配置修改。



Revision	Date/Time	Administrator	Comments
2	12/04/2006 15:05:09	admin	:39
1	12/04/2006 15:00:14	admin	:27

图8.4-2 修改控制页面

参数名称	参数说明
页面导航	如果存在不止一页的修改信息您可以使用页面的中的控制图标在页面中导航。这些功能图标的作用包括： ● 返回到第一页 ● 倒退一页 ● 设定跳到某页 ● 前进一页 ● 到最后一页

修改	表示配置被保存顺序的递增编号。如果一项或多项配置被删除后,这些编号可能不是连接的。列表中排列在首位的是最近的修改编号,也是最大的编号。
日期/时间	现实保存配置时的日期与时间。
管理员	显示备份该修改版本的管理员。
注释	有关保存配置的相关描述性信息可以说明修订版本被保存的原因、保存操作的管理员,以及为了释放空间修改版本被删除的时间。
差异图标	点击比较两个版本的差异。 点击该图标后将打开一个比较对话框: ● 当前配置 ● 从显示列表中选中的修改版本,包括修改的历史纪录与模板。 ● 指定修改版本号。
下载图标	点击将选中的修订版本下载到本地 PC。
恢复图标	点击返回到所选的修改版本系统将弹出提示符询问是否确认这样的操作。

有关系统维护 US Service、配置恢复与备份的详细信息,参见“系统配置维护”。

8.5 设置

进入系统>管理员设置>设置，设置以下选项：

- HTTP 与 HTTPS 管理访问的端口
- 超时设置，包括闲置超时
- 显示设置，包括基于 web 管理器使用的语言与生成报告中显示的行数
- LCD 与控制键的 PIN 保护（只适用于安装了 LCD 的设备型号）
- 对通过 SSH 登录的用户启动 SCP 功能

管理员设置

Web管理接口

HTTP 80

HTTPS 443

SSLVPN登录端口 10443

Telnet端口 23

SSH端口 22

启动与1.0版本兼容

超时设置

超时控制 480 (1-480 分)

显示配置

语言版本 简体中文

行数/每页 50 (20 - 1000)

GUI中支持配置IPv6

LCD 面板管理

激活PIN保护 (PIN)

启用SCP

图8.5-1 管理员设置

参数名称	参数说明
Web 管理端口	
HTTP	输入用于 HTTP 管理访问的 TCP 端口。默认端口是 80。
HTTPS	输入用于 HTTPS 管理访问的 TCP 端口。默认端口是 443。
Telnet 端口	输入用于管理访问的 telnet 端口。默认端口是 23。
SSH 端口	输入用于管理访问的 ssh 端口。默认端口是 22。
启动 **v1** 兼容	启动除 v2 之外，与 SSH v1 的兼容性。
闲置超时	设置系统管理员必须再次登录之前，系统的闲置超时时间。上限的超时时间为 480 分钟（8 个小时）。为了提高安全性，系统默认的闲置时间为 5 分钟。
显示设置	

语言	选择基于 web 管理器使用的语言。可选的语种为：英语，简体中文，日语，韩语与法语。 您应该选择管理计算机操作系统使用的语言。
每页显示行	设置列表中每页显示的行数。默认是 50。设置范围是 20 到 1000。
LCD 面板（只适用于安装了 **LCD** 的设备型号）	
激活 **PIN** 保护	点击密码保护的检查框，输入 6 位的密码。管理员必须输入该密码使用控制按键与 LCD。参见，“设置 LCD 面板密码保护”。
启动 **SCP**	如果您想使用户通过 SSH 登录，启动使用 SCP 复制配置文件。

注意：如果您将默认的端口更改为 http、http、telnet、或 SSH，请确定端口号是唯一的。

8.6 监控管理员

基于 web 管理器页面的状态栏中显示登录的管理员数量。系统信息项下，您可以查看当前的管理员。点击“详情”查看当前登录 ZXSEC US 设备的管理员信息。

管理员登录 - Microsoft Internet Explorer

刷新　　关闭

	用户名称	类型	来自	时间
☐	pengxl	sshv2	10.16.33.185	Fri Jun 6 09:04:13 2008
☐	admin	https	10.16.26.100	Fri Jun 6 09:03:49 2008
☐	lilj	https	10.16.26.180	Fri Jun 6 09:05:22 2008
☐	user	https	10.16.27.120	Fri Jun 6 09:06:05 2008
☐	admin	jsconsole	N/A	Fri Jun 6 09:06:09 2008

图8.6-1　系统信息>当前管理员

系统状态

序列号	US20103607501242
持续运行时间	0 天 15 小时 42 分钟
系统日期	Fri Jun 6 09:17:34 2008
HA状态	主动-主动
集群名称	US-HA
集群成员	US20103607501242/US20103607501242(主)
软件版本	US2010 3.00-b0650(MR6)
US Desktop 版本	
运行模式	NAT
虚拟域	Disabled 禁用
当前管理员	5 [查看]

图8.6-2　监控窗口显示的登录管理员列表

参数名称	参数说明
断开连接	点击该按键，断开所选的管理员的连接。只有对系统配置具有写的权限才可以使用该功能。
刷新	点击刷新列表。
关闭	点击关闭该窗口。
功能框	选中每个管理员对应的功能框后，点击“断开连接”可以将选中的管理员退出连接。只有对系统配置具有写的权限的管理员才可以执行该操作。默认的 admin 用户不能退出登录。
用户名	管理员的帐户名称。
类型	访问类型：使用基于 web 的管理器或 CLI。
来自	如果类型显示为“WEB”，那么该栏目显示的是管理员使用的 IP 地址。 如果类型显示为“CLI”，那么该栏目是 SSH 或 telnet，管理员使用的 IP 地址或 Concole
时间	管理员登录设备的时间与日期。

第9章 系统维护

9.1 概述

描述

本章是有关如何备份与恢复系统配置以及如何配置从 US SERVICE 中心（US Service Distribution etwork）获得自动更新的内容。

内容

9.2 系统配置维护

进入系统>维护>备份与恢复，备份与恢复系统配置以及进行固件管理。您可以将系统配置文件包括网页内容过滤文件与垃圾邮件过滤文件备份到管理计算机中或那些支持 USB 硬盘设备的 USB 硬盘中。您可以从上述的备份地址或备份文件中恢复系统配置。

如果您想所备份的文件包括 VPN 证书，您必须启动备份文件加密。当启动虚拟域配置后，虚拟域的备份文件内容取决于属于该虚拟域的管理员。

从 admin 管理员账户备份的系统文件包含全局设置以及每个 VDOM 的设置。也只有 admin 管理员可以恢复该配置文件。当您从一个普通管理员账户备份系统文件时，备份文件包含全局配置以及该普通管理员所属的 VDOM。只有普通管理员账户恢复该配置文件。

备份与恢复配置拆分为几个部分，分别进行说明。这些部分包括：

- 备份与恢复
- 固件
- US Desktop
- 固件升级
- 高级选项

备份与恢复

您可以设置将系统配置备份以及恢复备份的配置。

备份与恢复都具有集中管理选项。使用集中管理，您必须先在“系统>Admin”中配置使用集中管理选项。

备份与恢复---本地选项



图9.2-1 备份与恢复---本地选项

固件管理

固件显示ZXSEC US设备当前安装的固件版本如果您的设备中存储了不止一个固件镜像，该栏目中还将显示当前您所使用的固件镜像。

固件管理

系统

分区	活动	最后一次升级	系统版本
1	✔	N/A	US2010-3.00-US-build660-080505
2	✖	N/A	US2010-3.00-US-build650-071224

图9.2-2 固件管理

参数名称	参数说明
分区	一个分区可以包含一个版本的固件与系统配置。
状态	呈现绿色对勾表示这个分区所包含的固件与配置文件当前是使用状态。
最近升级日期	该分区最近一次升级的时间。
固件版本	ZXSEC US固件版本与子版本号。您可以使用备份分区： ● 点击“上传”从管理计算机或ZXSEC USB硬盘替换固件。 ● 点击“上传并重启”替换固件并激活该分区。

参数名称	参数说明
使用固件重新启动 **ZXSEC US** 设备	使用备份的固件重新启动 ZXSEC US 设备。

固件升级

固件升级中显示通过 US Service 网络升级固件的选项，这样的功能选项只有完成设备注册后才是可用的。

固件升级

通过文件升级： 浏览. . .

确定

图9.2-3 固件升级

参数名称	参数说明
升级方式	通过 US Service 网络升级固件的版本。
（选择）	选择可用的固件版本。
允许固件降级	选择安装较当前版本旧的固件版本安装。 这样的选择在当前的固件版本更改导致您所需要的功能不可用的情况下，您可以选择恢复为旧的版本。
通过文件升级	点击“浏览”从本地 PC 选择文件上传到 ZXSEC US 设备。
确定	点击“确定”确认选项。

高级选项

高级选项包括 USB 自动安装功能、执行 CLI 命令以及调试日志功能。

高级(USB自动安装，输入命令行，下载调试日志)

USB自动安装

在系统重启时，如果USB盘上有缺省的文件名那么会自动升级ZXSEC US配置文件.

缺省的配置文件名： US2010.conf

在系统重启时，如果USB盘上有缺省的文件名那么会自动升级ZXSEC US系统.

缺省的文件名： image.out

图9.2-4 高级选项

参数名称	参数说明
高级选项USB 自动安装）	只有 ZXSEC US 设备与 USB 硬盘连接时可用。根据需要设置选项并重新启动 ZXSEC US 设备。

参数名称	参数说明
	如果您同时选择了更新配置与固件升级选项那么系统在重新启动时同时完成以上两项任务。ZXSEC US 设备将不再重新下载已经下载的固件或配置文件。
系统重启时自动更新 **ZXSEC US** 配置文件	系统重启时自动更新 ZXSEC US 配置文件。请确认默认的配置文件名称与 USB 硬盘中的配置文件名称相匹配。
系统重启时自动更新 **ZXSEC US** 固件	系统重启时自动更新 ZXSEC US 配置文件。请确认默认的镜像名称与 USB 硬盘中的镜像名称相匹配。
输入主要的命令行	从管理计算机的文本文件中将网址过滤与垃圾邮件过滤导入到 ZXSEC US 设备。输入文件名与路径或点击"浏览"确定文件存储的位置。 您可以通过引用配置备份文件中适当的文件或输入对应的 CLI 命令创建文本文件。
下载调试日志	下载到加密的调试日志。您可以将该调试日志发送到中兴通讯技术支持中心协助您诊断 ZXSEC US 设备出现的问题。

USB 硬盘

US 设备配置了 USB 接口，支持使用 USB 硬盘备份与恢复配置。

ZXSEC US 设备支持专用 USB 与通用的 USB。但是 USB 硬盘的格式必须是 FAT16 磁盘格式。不支持其他的分区类型。



注意：

格式化 USB 将删除 USB 中所有的信息。当 USB 与 ZXSEC US 设备连接时，在命令行提示符中输入 exe usb-disk format 格式化 USB。

当 USB 与 Windows 系统连接时在 DOS 命令行提示符中输入 format <drive_letter>:

/FS:FAT /V:<dirive_label>。<drive_letter>中的"letter"是您设置连接的 USB 驱动的格式，<dirive_label>中的"label"是设定识别 USB 的名称。

9.3 US Service 中心

您可以配置 ZXSEC US 设备连接到 US Service 并享有 US Service 中心提供的服务。US Service 提供反病毒与供给定义的更新。US Service 中心提供的服务包括在线 IP 地址黑名单、URL 黑名单与其他垃圾邮件过滤工具。

US Service

US Service 提供反病毒（包括灰色软件)以及 IPS 攻击定义的更新。当 ZXSEC US 连接到 US Service 时，根据 ZXSEC US 设备的设置的时区连接到最近的 US Service 服务器。

ZXSEC US 设备支持以下更新功能：

- 用户向 US Service 中心服务器发起的更新。
- 设定以每小时，每天或每星期的时间表从 US SERVICE 中心更新反病毒与攻击定义与反病毒引擎。
- 推进式更新。
- 更新状态包括版本号，过期时间，与更新日期与时间。
- 通过 NAT 设备进行推进式更新。

接收更新之前，您必须在中兴通讯指定的网站对所购买的 ZXSEC US 设备进行注册。参见“US 设备注册”。

根据所设定的时间接收更新之前，ZXSEC US 设备需要通过端口 443 使用 HHTPS 连接到 US SERVICE 中心。有关配置定期更新的时间设置，参见“启动更新时间表”。

您也可以配置 ZXSEC US 设备接收推进式更新。ZXSEC US 设备接收推进式更新时，US SERVICE 中心必须使用 UDP 端口将数据包路由到 ZXSEC US 设备。有关配置推进式更新的详细信息，参见“启动推进式更新”。

US Service 服务

US Service 服务站点遍及全世界范围。中兴通讯公司可以根据需要增加与调整站点。

默认情况下，ZXSEC US 设备与相对最近的服务站点通讯。如果因为任何原因，连接不到最近的站点，ZXSEC US 设备将联系其他服务站点，其他相对近的站点将在几秒钟内列出。默认情况下，ZXSEC US 设备使用端口 53 通过 UDP 与服务站点建立通信连接。或者进入系统管理>维护>US Service 中心，设置端口 8888 通过 UDP 也可以用作与服务站点进行连接。

使用 CLI 命令 system US Service 中的 hostname 关键字可以更改默认的 US Service 服务站点主机名称。使用基于 web 的管理器不能更改 US Service 服务站点的名称。

有关 US Service 服务的详细信息，参见 US Service 服务中心页面。

US Service 反垃圾服务

US Service 反垃圾服务是中兴通讯公司提供的反垃圾邮件服务系统，包括 IP 地址黑名单、URL 黑名单以及垃圾邮件过滤工具。IP 地址黑名单中包含已知的生成垃圾邮件的邮件服务器的 IP 地址。URL 黑名单包含在垃圾邮件中发现的 URL。

US Service 反垃圾邮件系统是中兴通讯公司提供并配置的自动垃圾邮件识别与处理系统。US Service 反垃圾邮件系统保持持续的监控与动态更新，确保了系统提供最准确的服务。在防护墙保护内容文件中可以启动或撤消 US Service 反垃圾服务。详细信息，参见"垃圾邮件过滤选项"。

每台 ZXSEC US 设备都享有 30 天的 US Service 反垃圾邮件服务试用许可证。US Service 反垃圾邮件许可证是通过中兴通讯公司的服务器进行管理的，不需要输入许可证信息。当启动 US Service 反垃圾邮件服务后，ZXSEC US 设备将自动与 US Service 反垃圾邮件服务站点进行通信连接。免费试用期结束后，联系中兴通讯技术支持中心续续延使用期限。

进入系统管理>维护>US Service 中心，可以整体上启动 US Service 反垃圾服务然后在每项防火墙保护内容文件中配置垃圾邮件过滤选项。参见"垃圾邮件过滤选项"。

US Service 网页过滤服务

US Service 网页过滤服务是中兴通讯公司推出的可管理性的网页过滤服务解决方案。US Service 网页过滤服务将数百万的网页分为设定的一些类型范围，用户可以对过滤不同分类的网页采取允许通过，屏蔽以及监控的动作。ZXSEC US 设备访问最近的 US Service 网页过滤服务器以识别所请求网页的类型，然后遵循对该用户或接口配置的防火墙策略。

每台 ZXSEC US 设备都享有 30 天的 US Service 网页过滤服务试用许可证。US Service 网页过滤许可证是通过中兴通讯公司的服务器进行管理的，不需要输入许可证信息。当启动 US Service 网页过滤服务后，ZXSEC US 设备将自动与 US Service 反垃圾邮件服务站点进行通信连接。免费试用期结束后，联系中兴通讯技术支持中心续续延使用期限。

进入系统管理>维护>US Service 中心，可以整体上启动网页过滤服务然后在每项防火墙保护内容文件中配置垃圾邮件过滤选项。参见"US Service 网页过滤选项"。

配置 US 设备与 US SERVICE 中心连接以及 US Service 服务

进入系统管理>维护>US Service 中心，配置从 US SERVICE 中心获得更新与 US Service 服务。更新中心包括三个方面的功能实现：

- 支持合同与 US Service 订购服务
- 反病毒与 IPS 下载
- Web 过滤与反垃圾选项

支持合同与 US Service 订购服务

支持合同与 US Service 订购服务板块可以在系统状态页面收缩的形式显示。

US Service 分布网络
服务合同
可用性 不能建立连接
US Service 定制服务
防病毒 不能建立连接
病毒库 8.631 (升级 2008-01-15 via 手工升级)
扩展设置 0.000 (升级 2003-01-01 via 手工升级)
入侵防御 不能建立连接
IPS库 2.442 (升级 2007-11-08 via 手工升级)
Web过滤 不能建立连接
反垃圾邮件 不能建立连接
管理服务 不能建立连接
反病毒与IPS选项
Web过滤和反垃圾邮件选项

图9.3-1 支持合同与 US Service 订购服务板块

参数名称	参数说明
支持合同	ZXSEC US 设备支持合同的状态或可用性。 所显示的状态可以是：不可达、未注册或有效合同。如果显示有效的合同，那么同时也显示 USOS 版本、合同的有效期以及支持的级别信息。
注册	点击注册 ZXSEC US 设备支持合同。该选项只有在支持合同没有被注册时显示。
US Service 订购服务为	每项 US Service 订购服务的可用性与状态，包括： ● 反病毒 AV 定义 入侵防护 IPS 定义 ● Web 过滤 ● 反垃圾服务 ● 管理服务 ● 分析服务

可用性	根据您订购的服务情况，ZXSEC US 设备中这些服务的可用性。状态显示可以是：不可达、未注册、有效许可证或有效合同。如果可用性显示为“未注册”，将出现订购选项。如果可用性显示为“过期”，将出现更新选项。
状态图标	图标显示的颜色表示订购服务的状态。 ● 灰色；表示不可达，ZXSEC US 设备不能连接到服务。 ● 黄色；表示未注册，ZXSEC US 设备可以连接，但是对于这项服务没有注册的合同支持。 ● 黄色；表示过期，ZXSEC US 设备的有效许可证已经过期。 ● 绿色；表示有效许可证，ZXSEC US 设备可以连接到 US SERVICE 中心并具有已经注册的支持合同。 如果状态图标呈绿色，同时显示过期时间。
版本	当前安装在 ZXSEC US 设备中用于 US Service 服务的定义文件的版本号。
最近一次更新日期与方式	最近一次下载更新定义文件的时间以及方式。
[更新]	点击进行手动更新。该操作将您转到从本地计算机下载更新文件。从 US SERVICE 中心直接下载更新，点击“立即更新”。
（日期）	ZXSEC US 设备最近一次查看更新时，本地系统显示的时间。
反病毒与 **IPS** 更新	点击蓝色箭头显示或隐藏该栏目。
Web 过滤与反垃圾邮件选项	点击蓝色箭头显示或隐藏该栏目。
IPS 选项	点击蓝色箭头显示或隐藏该栏目。 点击将攻击的详细信息发送到 FSN，以提高 IPS 特征质量。 中兴通讯公司建议您启动该功能，将攻击信息发送到 FSN。
管理与分析服务选项	点击蓝色箭头显示或隐藏该栏目。 输入注册 ZXSEC US 设备使用该服务时，获取的帐户 ID。如果 ZXSEC US 设备没有与 USLA 设备连接或注册使用 US Service 分析服务，该栏目中没有任何内容显示。 如果您没有帐户 ID，使用用户服务注册 US Service 管理服务。
反病毒与 **IPS** 更新下载	点击反病毒与 IPS 下载栏目旁边的蓝色箭头，扩展该选项。在您启动推进式更新包括输入与 US SERVICE 中心服务连接的接口的 IP 地址时，ZXSEC US 设备。将发出 SETUP 信息 如果您配置使用的 ZXSEC US 设备位于 NAT 设备之后将使用“使用代理推进选项”该选项创建一项策略，将流入的 FDS 流量重新定向到 ZXSEC US 设备。ZXSEC US 设备发送 NAT 设备的 IP 地址与端口数量到 FDS。但是，NAT 设备同时也必须配置通过端口 9443 将 FDS 流量转发到 ZXSEC US 设备。 详细信息，参见“通过 NAT 设备启动推进更新”。

反病毒与 IPS 选项

反病毒与IPS选项

使用强制服务器地址

允许服务器推送式升级

使用强制推动升级IP地址　端口 9443

定期升级

全部 1 (小时)

每天: 0 (小时)

每周: Sunday (天) 0 (小时)

提交攻击特征给US Service服务网络以改善IPS特征质量（推荐）

图9.3-2　反病毒与 IPS 选项

参数名称	参数说明
使用代理服务器地址	如果不能与 US SERVICE 中心连接或您的公司使用自有的 USProtect 服务器更 新反病毒与攻击定义与引擎，您可以配置代理服务器。选中“使用代理服务器地址”功能框并输入 USProtect 服务器的 IP 地址或域名，并点击“应用”。如果 US SERVICE 中心状态仍然显示没有到 US SERVICE 中心的连接，参见“US SERVICE 中心连接故障检修”。
允许推进式更新	点击允许推进式更新。推进式更新是指只要存在可用的更新，即使您不查看，服务器也将自动将可用的更新发送到 ZXSEC US 设备。推进式更新的状态图标可以显示推进更新服务的状态。
推进式更新状态图标	接收推进式更新时，ZXSEC US 设备的状态： ● 灰色，表示不可达，ZXSEC US 设备不能连接到推进更新服务器。 ● 黄色，表示不可用，当前支持许可证的情况下推进式更新服务不可用。 ● 绿色，表示可用，允许推进式更新服务。 如果状态图标显示灰色或黄色，参见“US SERVICE 中心连接故障检修”。
使用代理推进更新	如果 US 设备与 FDS 之间存在 NAT 设备，启动代理推进更新。代理推进更新允许您创建转发策略将进入的 FDS 更新重新定向到 US 设备。 需要配置 NAT 设备，包括 UDP 端口 9443，将 FDS 流量转发到 US 设备。
IP 地址	输入位于 ZXSEC US 设备之前的 NAT 设备的 IP 地址。当 FDS 试图发送流量到达 ZXSEC US 设备之前，将要与 NAT 设备连接。 该选项只有在“使用代理推进更新”功能启动后可用。

	设置 NAT 设备接收 FDS 发送的推进更新的端口。该端口必须转发到 ZXSEC US 设备中的 UDP 端口 9443。 该选项只有在“使用代理推进更新”功能启动后可用。
更新时间设置	选中功能框启动该项功能。
间隔时间	设置间隔多少小时（1 到 23 小时之间）尝试更新连接。选择每次更新请求发送的间隔时间。
每天	每天发送更新请求。您可以指定一天中检查更新的时间点。在指定的时间内会随意的发起更新连接。
每周	每周发送更新请求。您可以指定一个星期中的任何一天中的任何时间发起更新连接。在指定的时间内会随意的发起更新连接。
立即升级	点击该选项手动发起更新。

Web 过滤与反垃圾邮件选项点击 Web 过滤与反垃圾邮件选项旁边的蓝色箭头，扩展该选项。

Web 过滤与反垃圾邮件选项

Web过滤和反垃圾邮件选项

Web过滤

启用缓存 TTL: 3600

反垃圾邮件

启用缓存 TTL: 1800

端口选择

使用默认端口(53).

使用自定义端口(8888).

连接测试

(US Service服务不能启用.)

图9.3-3 Web 过滤与反垃圾邮件选项

参数名称	参数说明
启动 **web** 过滤	选中“启动 US Service web 过滤服务”功能框，启动该服务。
使用缓存	选中“启动缓存”功能框，启动缓存 US Service 服务信息。 该功能通过减少 US 设备对 US Service 服务器的请求次数提高了访问速度。配置的缓存空间占 ZXSEC US 设备内存的 6%。如果暖存满了，最近使用的 IP 地址或 URL 都将被删除。 该功能只有在“启动 US Service web 过滤服务”的情况下可用。
TTL	存活时间。在与服务器再次连接之前将被屏蔽的 IP 地址与 URL 存储在缓存的时间，以秒计。 该功能只有在“启动 US Service web 过滤服务”的情况下可用。
启动反垃圾邮件	选中“启动 US Service 反垃圾邮件服务”功能框，启动该服务。

使用缓存	选中"启动缓存"功能框，启动缓存 US Service 服务信息。 该功能通过减少 ZXSEC US 设备对 US Service 服务器的请求次数提高了访问速度。配置的缓存空间占 ZXSEC US 设备内存的 6%。如果缓存满了，最近使用的 IP 地址或 URL 都将被删除。 该功能只有在"启动 US Service 反垃圾邮件服务"的情况下可用。
TTL	存活时间。在与服务器再次连接之前将被屏蔽的 IP 地址与 URL 存储在缓存的时间，以秒计。 该功能只有在"启动 US Service 反垃圾邮件服务"的情况下可用。
使用默认端口（53）	点击使用端口 53 与 US Service 反垃圾邮件服务器进行通讯。
使用备用端口（8888）	点击使用端口 8888 与 US Service 反垃圾邮件服务器进行通讯。
检测连接性	点击该按键检测与 US Service 反垃圾服务器的连接。检测结果显示在该功能键下边。
请点击这里	点击重新评估 US Service web 过滤服务中 URL 分类结果。

管理与分析服务选项用于配置 US Service 管理与日志&分析服务。点击日志与服务选项旁边的蓝色箭头扩展该选项。

检修与 US SERVICE 中心的连接故障

如果 ZXSEC US 设备连接不到 US SERVICE 中心，请检查连接配置。例如，在 ZXSEC US 设备路由表中添加路由或配置您的网络允许 ZXSEC US 设备使用通过端口 443 使用 HTTPS 连接到互联网。

您可能需要连接到一个代理 US Service 服务器去获得更新。参见"添加代理服务器"。如果连接还是不成功，检查您的配置确保可以从 ForitGate 设备连接到代理 US Service 服务器。

推进式更新在以下情况下不可以获得：

- 您没有进行设置注册。（参见"ZXSEC US 设备注册"）
- ZXSEC US 设备与 US SERVICE 中心之间安装了 NAT 设备。（参见"通过 NAT 启动推进式更新"）
- ZXSEC US 设备使用代理服务器与互联网连接。（参见"通过代理服务器启动更新时间表"）

更新反病毒与攻击定义

使用以下步骤配置 ZXSEC US 设备连接到 USProtect Distribution Network（US SERVICE 中心）更新反病毒（包括灰色软件）定义，入侵攻击定义与引擎。

确定 **ZXSEC US** 设备连接到了 **US SERVICE** 中心

1. 进入系统管理>状态，点击系统信息区域的系统时间中的“更改”。
2. 确定 US SERVICE 中心的时区选择与 US 设备设置的时区相符。
3. 进入系统管理>维护>US Service 中心。
4. 点击“刷新”。

ZXSEC US 设备检验与 US SERVICE 中心的连接。检验结果显示在系统更新页面的顶部。

更新反病毒与攻击定义

1. 进入系统管理>维护>US Service 中心。
2. 点击“立即更新”更新反病毒与攻击定义与引擎。如果与 US SERVICE 中心或代理服务器的连接正常，基于 web 的管理器显示类似以下的信息：Your update request has been sent. Your database will be updated in a few minutes.

Please check your update page for the status of the update.

几分钟后，如果有可用的更新，系统更新中心页面将列出新版本的反病毒定义，反病毒引擎与攻击定义或引擎的信息。系统状态页面同样显示更新的日期与更新文件的版本号。事件日志将记录更新信息的状况显示更新是否成功。

注意:反病毒与攻击定义更新的时候会导致 ZXSEC US 设备应用新的特征数据库时流量扫描暂短中断的可能性。为了尽量避免这样的可能性，设置更新是以较小的流量进行。

设置更新时间

1. 进入系统管理>维护>更新中心。
2. 选中“设置更新时间”的功能框。
3. 选择以下更新的频率以及下载更新的时间。

参数名称	参数说明
间隔时间	设置间隔多少小时（1 到 23 小时之间）尝试更新连接。
每天	每周发送更新请求您可以指定一个星期中的任何一天中的任何时间发起更新连接。
每周	每周发送更新请求您可以指定一个星期中的任何一天中的任何时间发起更新连接。

4. 点击“应用”ZXSEC US 设备将根据新设定的更新频率执行更新任务。

只要 ZXSEC US 设备执行设置的更新频率，事件日志中都将进行记录。

添加代理服务器如果 ZXSEC US 设备连接不到 US SERVICE 中心，或您的公司使用其自己的 USProtect 服务器器提供反病毒与攻击更新，您可以使用以下步骤添加代理 USProtect 服务器的 IP 地址。

1. 进入系统管理>维护>US Service 中心。
2. 选中“使用代理服务器 IP 地址”的功能框。
3. 输入有效的域名或 USProtect 服务器的 IP 地址。
4. 点击“应用”。

ZXSEC US 设备检验与代理服务器的连接。应用了代理服务器地址后，便可以更改 USProtect Distribution Network 设置，ZXSEC US 设备便与代理服务器建立了连接。如果 USProtect Distribution Network 设置显示为“不可用”，ZXSEC US 设备将不能与代理服务器连接。查看 ZXSEC US 设备的配置与网络设置确定通过 ZXSEC US 设备可以连接到代理 USProtect 服务器。

通过代理服务器启动更新时间如果 ZXSEC US 设备必须通过代理服务器连接到互联网，您输入输入 config system autoupdate tunneling 命令允许 ZXSEC US 设备通过代理服务器与连接到 US SERVICE 中心。有关 config system autoupdate tunneling 命令的详细信息，参见 ZXSEC US 设备 CLI 使用参考手册。

启动推进式更新

US SERVICE 中心发送推进式更新到 ZXSEC US 设备对比较严重的病毒或攻击情况作出快且到位的回应。ZXSEC US 设备接收推进更新之前必须进行了设备注册。参见“US 设备注册”。

当您配置 ZXSEC US 设备允许接收推进更新时，ZXSEC US 将发送 SETUP 信息到 US SERVICE 中心。下一次发布新的反病毒引擎，反病毒定义以及新的攻击定义与引擎的时候，US SERVICE 中心通知所有配置接收推进更新的 ZXSEC US 设备有可用的新的更新。接收更新通知的 60 秒内，ZXSEC US 设备从 US SERVICE 中心获得更新要求



注意：

如果 ZXSEC US 设备必须通过代理服务器与 US SERVICE 中心连接便不支持推进式更新。详细信息，参见“通过代理服务器启动更新时间表”。

网络配置允许，除了配置设定更新时间外，建议配置推进式更新功能。平均起来，ZXSEC US 设备接受 US SERVICE 中心发起的推进式更新比设定的更新时间要快。但是，设定的更新时间能够确保 ZXSEC US 设备接收最新的更新。

并不推荐将推进式更新设置为唯一获取更新的方法。ZXSEC US 设备有接收不到 US SERVICE 中心发送的更新通知信息的可能也有可能当 ZXSEC US 设备接收到被动更新通知时，只尝试发起一次与 US SERVICE 中心的连接与下载更新文件。

设置推进式更新

1. 进入系统管理>维护>US Service 中心。
2. 点击“允许推进式更新”。
3. 点击“应用”。

ZXSEC US 设备 **IP** 地址更改时启动推动式更新当启动了推进更新，那么必须设置 US SERVICE 中心连接 ZXSEC US 设备的接口，ZXSEC US 设备将发送 SETUP 信息包括设备接口的 IP 地址到 US SERVICE 中心。如果 ZXSEC US 设备运行于 NAT/路由模式，根据不同的设备型号，SETUP 信息中将包括接口的 IP 地址。如果设备运行于透明模式，SETUP 信息中将带有 ZXSEC US 管理 IP 地址。US SERVICE 中心必须能够连接到该 IP 地址，ZXSEC US 设备才能够接收到推进更新信息。

当您手动更改该接口的 IP 地址时，或将该接口的询址模式设置为 DHCP 或 PPPoE 时，以及 PPPoE 服务器更改 IP 地址时，ZXSEC US 设备将发送新的 SETUP 信息告知 US SERVICE 中心接口地址更改的情况。

设备 ZXSEC US 设备接收推进式更新之前，US SERVICE 中心必须能够连接到该 IP 地址。如果 ZXSEC US 设备位于 NAT 设备之后，参见“通过 NAT 设备启动推进式更新”。

如果您设置冗余连接可以访问互联网当其中一项连接失败以及 ZXSEC US 设备通过其它的互联网连接方式故障时，ZXSEC US 设备也会发送 SETUP 信息。

透明模式下，如果您更改了管理 IP 地址，ZXSEC US 设备也同样发送 SETUP 信息告知地址更改的状况。

通过 **NAT** 设备启动推进式更新如果 US SERVICE 中心只有通过 NAT 设备连接到 ZXSEC US 设备，您须在 NAT 设备上配置端口映射并将端口映射信息添加到推进式更新配置。设置端口映射后，US SERVICE 中心既可以使用端口 9443 也可以使用您指定的代理端口连接到 ZXSEC US 设备。

注意：如果 NAT 设备的外部 IP 地址是动态的（例如，设置使用了 PPPoE 或是 DHCP），ZXSEC US 设备则不能通过 NAT 设备接收被动更新。

通过 NAT 设备进行推进式更新（举例网络结构）

常规操作

使用以下步骤配置内部网络的 US NAT 设备与 ZXSEC US 设备使得内部网络中的 ZXSEC US 设备能够接收推进式更新：

1. 在内部网络注册 ZXSEC US 设备并获得许可证信息,以便能够接收推进式更新。

2. 在内部网络中配置 ZXSEC US 设备中的 US Service 中心选项。

- 允许推进式更新
- 添加代理推进更新的 IP 地址。通常情况下，该 IP 地址时 NAT 设备的外部接口的 IP 地址。
- 如需要，更改代理推进更新端口。

3. 配置 NAT 设备的端口转发虚拟 IP。

- 设置虚拟 IP 的地址为外部 IP 地址，且与代理推进更新的 IP 地址相匹配。通常情况下，该 IP 地址时 NAT 设备的外部接口的 IP 地址。

4. 在 US NAT 设备中添加防火墙策略，包括端口转发虚拟 IP 地址。

在内部网络中配置 ZXSEC US 设备中的 US Service 中心选项

1. 进入“系统>维护>US Service 中心”。

2. 点击“允许推进式更新”。

3. 点击“使用代理推进更新 IP”并输入 NAT 设备外部接口的 IP 地址。

4. 除非 UDP 端口 9443 被屏蔽或被网络中其它服务占用，否则不要更改推进更新端口。

5. 点击“应用”。

ZXSEC US 设备发送代理推进 IP 地址与端口到 US SERVICE 中心。US SERVICE 中心便使用该 IP 地址与端口将推进式更新发送到 ZXSEC US 设备。推进式更新的真正实现还在于，配置 NAT 设备的虚拟 IP 地址以便 NAT 设备在接收到推进式更新数据包时能够将数据包转发到内部网络中的 ZXSEC US 设备。



注意：

如果外部 IP 地址或外部服务端口发生更改，将更改信息添加到“使用代理更新”配置的选项中，点击“应用”更新 US SERVICE 中心中的推进更新信息。

配置 US NAT 设备添加转口转发虚拟 IP 地址配置 NAT 设备使用端口转发，将推进式更新连接从 US SERVICE 中心转发到内部网中的 ZXSEC US 设备。

1. 进入“防火墙>虚拟 IP”并点击“新建”。

2. 添加端口转发虚拟 IP 地址，将 NAT 设备的外部接口影射到内部网络中 ZXSEC US 设备的 IP 地址，使用推进更新 UDP 端口。

参数名称	参数说明
名称	设置虚拟 IP 的名称。
外部接口	NAT 设备与互联网连接的接口。
类型	静态 NAT。
外部 **IP** 地址/范围	US SERVICE 中心连接内部网络中的 US 并发送推进式更新的地址。该地址通常是 NAT 设备外部接口的地址该地址必须与内部网络中 ZXSEC US 设备中 US Service 中心推进更新代理 IP 地址选项中配置的地址相同。
映射 **IP** 地址/范围	内部网络中 ZXSEC US 设备的 IP 地址。
端口转发	选择“端口转发”功能框。
协议	UDP
外部服务端口	US SERVICE 中心连接的外部服务端口通常用于推进式更新的外部服务端口是 9443。如果您在 ZXSEC US 设备的 USService 中心配置选项中更改了推进式更新端口，您必须相应更改外部服务端口。
映射到端口	映射到端口必须与外部服务端口相同。

3. 点击 OK 确认。

配置 US NAT 设备添加防火墙策略

1. 在内部防火墙策略中添加新的外部接口策略。

2. 配置策略。

3. 点击 OK 确认。

确认发送到内部网络中 ZXSEC US 设备的推进式更新已经生效

1. 进入“系统>维护>US Service 中心”。

2. 点击“刷新”。

推进更新状态图标应该保持持久的绿色显示。

9.4 许可证

如果您使用的 ZXSEC US 设备是 6000 系列或更高型号的该设备，您可以从中兴通讯公司购买许可证将 VDOM 的设置数量增加到 25，50，100 或 250。默认情况下，ZXSEC US 设备支持的最大 VDOM 的设置数量是 10 个。

许可证密钥是中兴通讯公司提供的 32 位的数列。中兴通讯公司需要您输入设备的序列号以便生成许可证密钥。

进入系统管理>维护>许可证，在弹出的对话框中输入许可证密钥。

设置另外 VDOM 所需的许可证密钥

参数名称	参数说明
当前许可证	当前设备的虚拟域的最大数量。
输入许可证密钥	输入中兴通讯公司提供的许可证密钥并点击“应用”。

第10章 静态路由

10.1 概述

描述

本章就如何定义静态路由以及创建路由策略内容进行了说明。

设置 ZXSEC US 设备的路由是指设置提供给 ZXSEC US 设备将数据包转发到一个特殊目的地的所需的信息。设置静态路由是将数据包转发到除了出厂默认的网关以外的目的地。

您可以从出厂配置的默认的静态路由中配置默认网关。您必须编辑出厂默认的路由,将 ZXSEC US 设备的路由指定为不同的默认网关;或删除出厂配置的路由并指定默认的静态路由到达默认的网关。（参见“默认的路由以及默认的网关”）

您也可以定义路由策略选项。路由策略中包含了检测流入数据属性的规则。使用路由策略,您可以配置 ZXSEC US 设备根据数据包包头的 IP 源感地址和目标地址以及其他规则，例如哪个接口接收数据包以及设置哪个端口用来传输数据包这样的规则来路由数据包。

内容

10.2 有关路由

路由是一个比较复杂的话题,一些人认为路由很难去把握并理解。ZXSEC US 作为网络中的安全设备，数据包必须通过该设备，您需要理解几条基本的路由涉及的概念以便正确的配置 ZXSEC US 设备。

不管您是小型还是大型网络的网管以下说明将有助您理解 ZXSEC US 设备如何执行路由功能。

包括以下内容：

- 如何创建路由表

- 路由路线的选择
- 多路线路由与最佳路由路线的选择
- 路由次序对路由优先性的影响
- 等同花费多路线路由（ECMP: equal cost multipath routes）
- 黑洞路由

如何创建路由表

出厂默认的配置下，ZXSEC US 设备路由表只包含一个默认静态路由设置。您可以通过定义其他的静态路由在路由表中添加路由信息。一个路由表中可能包含到同一个目的地的不同的路由，这些路由中指定中继路由的 IP 地址或与该路由发生通信的接口可能会不同。

ZXSEC US 设备通过评估路由表中的信息选择路由数据包的最佳路线。到一个目的地的最佳路由一般是 ZXSEC US 设备到最近的下一个中继路由之间的最短距离。在一些情况下，如果最佳路由因一些原因不可用，那么会选择相对其他路由最佳的路由。最佳路由将被添加在 ZXSEC US 转发列表中，转发列表是 ZXSEC US 路由表的子表。数据包将根据转发列表中的信息被转发。

路由路线的选择

每当一个数据包到达 ZXSEC US 设备中任何一个接口时，ZXSEC US 设备将通过使用该数据包包头含带的源 IP 地址做逆向查询以识别该数据包是否在合法的接口接收的。如果 ZXSEC US 设备通过接收该数据包的接口不能与计算机的源 IP 地址通信，那么 ZXSEC US 将认为这是黑客攻击的征兆而丢弃该数据包。

如果目标地址与本地地址能够匹配（并且本地配置允许数据包的传输），那么 ZXSEC US 设备将数据包传送到本地网络中。如果数据包的传输目的地是其它网络ZXSEC US 设备根据路由策略和/或存储在 ZXSEC US 转发路由表中的信息将把数据包转送在下一站中继路由（参见“路由策略”）。

多路线路由与最佳路由路线的选择

当路由表中几条进入的条目到达的是同一个目的地时，会发生多路径路由。多路径路由发生时，ZXSEC US 设备对进入的数据包可能存在几个可能的目标地址，迫使 ZXSEC US 设备判定哪个下一站中继是最佳的选择。

两种方法可以手动解决到达同以目的地存在多条路由路线的问题，一是降低其中一条路线的管理距离，二是设置路由路线的优先级。通往相同的网络地址的路由，

相对具有最短的管理距离的路由更为优越更可取。管理距离可以设置为 1 到 255 之间的人任何数值。

有关手动更改路由路线的优先级设置，如果 ZXSEC US 设备中存在两条道下一中继管理距离通向的路由，那么设备可能不能明确作出选择。通过配置路由的优先级使设备对路由作出选择。路由的优先级的设置只能通过 CLI 配置。优先级设置越低，越接近首选路由。

路由表中的所有条目都有对应的管理距离。如果路由表中包含的几个条目是指向同一个目的地时（这些条目可能具有不同的网关与接口通信设置），ZXSEC US 设备将各个条目的管理距离进行比较，选择具有最低管理距离的条目将其放置在 ZXSEC US 转发列表中作为路由路线。其结果是，ZXSEC US 转发列表中只包含具有最低管理距离到达各个可能的目的地的路由。更改静态路由的管理距离的有关信息，参见“在路由表中添加静态路由”。

路由次序对路由优先性的影响

ZXSEC US 设备根据静态路由的管理距离将其添加在转发路由表之后，这些路由的次序决定了路由的优先性。当转发路由表中存在到达统一目的地的两条路由时，具有最低次序号的路由被认为具有最高的路由优先权。

对于 USOS v3.0 系统来说，通过 CLI 可以设置路由的优先属性的字段。该字段可以忽略路由次序的设置，解决了具有相同管理距离的路由的选择问题，也就是说具有最高优先级设置的路由将成为首选路由。如果两条路由具有相同的优先级设置，将使用当前的方法解决。设置路由优先级的命令是 config route static 命令项下的 set priority<integer>。有关该命令的详细信息，参见 ZXSEC US 设备 CLI 使用参考手册。

当您通过基于 web 的管理器在静态路由列表中添加路由时，ZXSEC US 设备自动将下一个未分配的次序号分配给所添加的路由。例如，如图 144 所示，通过创建两条到达的是同一个目的地（1.1.1.0/24）的静态路由来说明基于 web 的管理器是如何分配路由次序号的。两条路由都指定了相同的网关，但是其中一条路由中，数据报是通过“端口 1”经过 ZXSEC US 设备的，另一条路由中，数据包则是通过“端口 2”经过 ZXSEC US 设备的。

新建

IP/掩码	网关	设备	路径长度	
0.0.0.0/0.0.0.0	10.16.13.3	port2	10	

图10.2-1 通过基于 web 的管理器创建的静态路由

因为条目 2 是先创建的，条目 3 是其次创建，那么在路由表中的次序编号分别为 2 与 3。当 ZXSEC US 设备衡量到达同一目的地的这两条路由时，因为其具有较低的管理距离，两条路由都将被添加在转发路由表中。添加在转发路由表之后，如果不通过 set priority 命令设置路由的优先级别，那么路由的次序号决定了其优先级。因为条目 2 具有较低的次序号，该路由将是首选的路由。



注意：

在 CLI 中输入 config router static，然后输入 get 将显示静态路由表中所有路由条目的次序号显示的次序号就是在定义静态路由时通过 edit<ID_integer>命令输入的数值。详细信息，参见 ZXSEC US 设备 CLI 参考手册中有关 config router static 命令的描述。

静态路由列表中的条目顺序也是通过基于 web 管理器在路由表中配置全部路由的次序。但是，当您使用 CLI 添加路由时可以指定静态路由的次序，路由的次序编号可能与其静态路由表中的条目编号不匹配。静态路由的次序编号只能通过 CLI 配置。总得来讲，如果路由表中的一个路由与到达同一目的地的另外一个路由相比较具有较低的次序号，ZXSEC US 设备将优先选择具有较低次序号的路由。因为您可以使用 CLI 指定次序号与优先级，当定义静态路由时，将根据路由的次序号与优先字段设置对相同目的地的路由进行选择。设定路由的优先级别，您必须使用 CLI 命令 config router static 创建路由并给该路由设置较低的次序编号与较高的优先级别。

等同花费多路线路由（ECMP: equal cost multipath routes）

到同一目的地存在不止一条路由路线时，便产生安装并使用哪条路由这样的问题。有关解决这样问题的方法，设置管理距离与路由优先级，在上文中有过叙述。但是，当这样的路由的管理距离与优先级设置都相同时，便成为等同花费多路线路由（ECMP: equal cost multipath routes）。如果对 ECMP 启动了负载平衡，那么不同的会话将使用不同的路由到达相同的地址。

黑洞路由

黑洞路由指丢弃所有发送到该路线进行路由的流量。类似 Linux 编程中的 /dev/null。

黑洞路由用于处理数据包而不是对可疑的查询作出回应。这样，原始发送端对于目标系统不暴露任何信息，从而增强了安全性。

黑洞路由也可以用于在子网中限制流量。如果一些地址不在使用状态，发送到这些地址的流量（这样的流量可能是有效的或恶意的）将被定向到黑洞路由从而增强了安全性并降低了子网中流量传输。

回环接口的添加可以简化黑洞路由的配置。如果一个虚拟接口不在转发流量，只能通过 CLI 配置这样的接口，配置如同常规的接口，但是这样的接口可供配置的参数较少且所有发送到该接口的流量将被停留在这里。这种情况的发生并不是因为硬件原因或链接状态的问题，那么接口总是处于可用状态。这样的接口同样也可以用于动态路由。经过配置后，回环接口可以应用防火墙策略、路由与其他配置。

10.3 静态路由

您可以通过定义数据包的目标 IP 地址与掩码配置 ZXSEC US 设备截取的数据包，并指定这些数据包的 IP 地址（网关）。网关地址是指数据包所到达的下一站中继路由。

注意：您可以使用 config router static6 CLI 命令添加、编辑或删除 IPv6 流量的静态路由。详细信息，参见 ZXSEC US 设备 CLI 参考手册中“路由”章节。

查看、创建并编辑静态路由

ZXSEC US 设备将数据包包头与静态路由列表中的信息相比较进行数据包路由。最初，列表中包含出厂配置的静态路由列表（参见“默认的路由与网关”）。其它的条目可以手动添加。

当您在静态路由列表中添加静态路由时，ZXSEC US 设备将衡量该路由信息与路由表中存在的其它路由相比较是否是不同的路由。如果路由表中没有路由具有相同的目的地，ZXSEC US 设备将表该路由添加在路由表中。

进入路由>静态>静态路由，可以查看静态路由列表。该选项下，点击路由条目对应的编辑图标可以编辑路由。

如下图所示属于一个具有“内部”与“外部”接口的 ZXSEC US 设备的静态路由表。您所管理的 ZXSEC US 设备的接口名称可能与该名称不同。

静态路由 策略路由

新建

IP/掩码	网关	设备	路径长度	
0.0.0.0/0.0.0.0	10.16.13.3	port2	10	

图10.3-1 静态路由列表

参数名称	参数说明
新建	添加新的静态路由。(参见“在路由表中添加静态路由”)
IP	ZXSEC US 设备所截取的数据包的传输的目标 IP 地址。掩码与该 IP 地址相通信的网络掩码。
网关	被截取的数据包所要转发的下一个中继路由的 IP 地址。
设备	路由数据包通过的 ZXSEC US 接口名称。
距离	路由的管理距离。其数值表示了到达下一站中继路由的距离。
删除、编辑图标	点击该图标可以删除，编辑的静态路由。

默认的路由与默认的网关

出厂默认的配置中,静态路由列表中条目 1 对应的目标地址是 0.0.0.0./0.0.0.0.,也就是说任何或全部的目标地址。该路由称为“静态默认路由”。如果路由列表中没有其它路由并且数据包需要经由 ZXSEC US 设备转发那么出厂配置的静态默认路由将使 ZXSEC US 设备将数据包转发到默认的网关。

ZXSEC US 设备使用最佳匹配算法路由数据包(忽略列表中的静态路由顺序)。配置数据包的路由,ZXSEC US 设备检测数据包的目标地址并通过路由表选择最佳匹配目标地址。如果发现相应的匹配，数据包将被转送到指定的网关。如果没有发现对应的匹配,ZXSEC US 将路由数据包到默认路由中指定的网关。默认路由的域值为 0.0.0.0/0.0.0.0(所有的目标地址)。根据默认路由的传送的数据包，您必须给默认的路由指定网关地址与向外的接口。

例如下图所示，ZXSEC US 设备与一台路由器连接。确保所有向外的数据包都能够通过路由器到达外部网络正确的地址，您必须编辑默认的配置并配置路由器是 ZXSEC US 设备的默认网关。

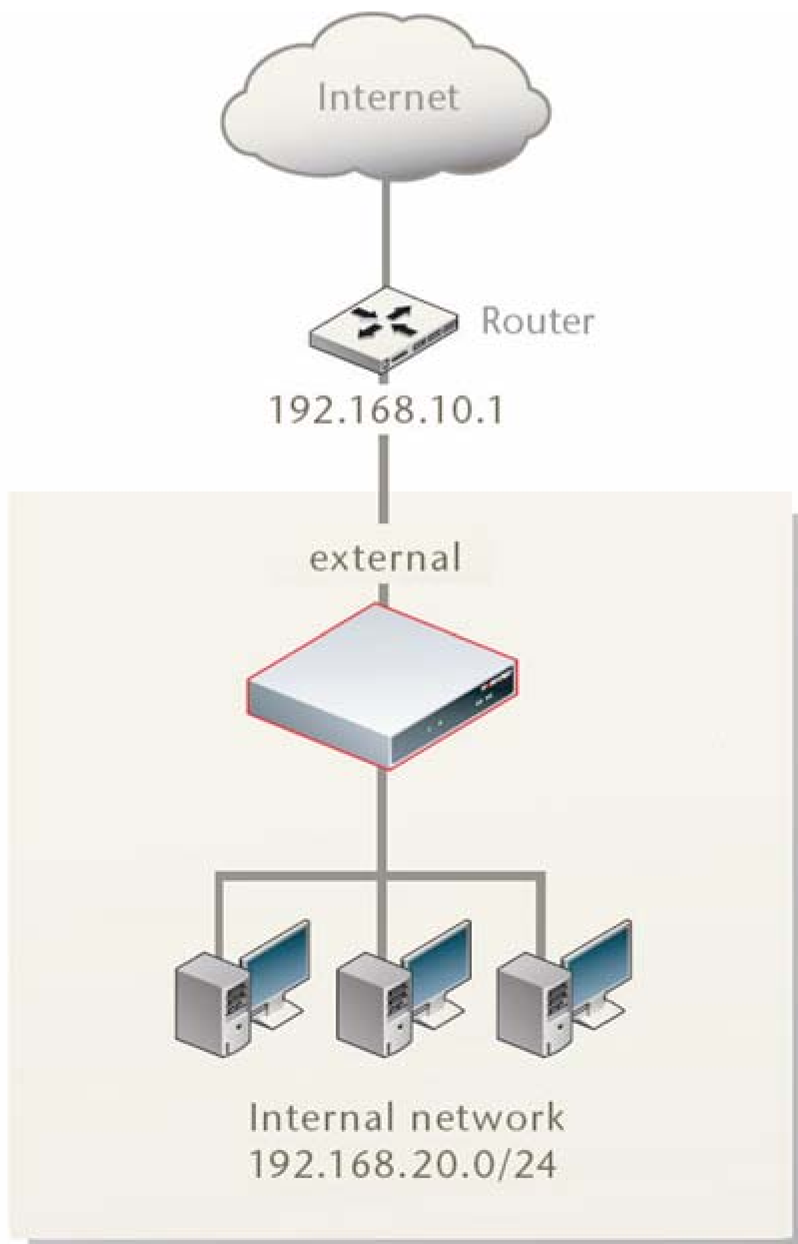


图10.3-2 配置路由器成为默认的网关

从内部网络将向外的数据包路由到不是网络 192.168.20.0/24 中的目标地址，您需要编辑默认的静态路由，包括进行以下设置：

- 目标 IP/掩码：0.0.0.0/0.0.0.0
- 网关：192.168.10.1
- 设备：与网络 192.168.10.0/24（例如外部接口）连接的接口名称

- 距离：10

网关设置是指定连接到 ZXSEC US 外部接口（External）的中继路由接口 IP 地址。位于路由器（192.168.10.1）之后的接口是 US_1 的默认网关。

如果数据包的目标 IP 地址并不在本地网络中而是在那些路由器之后的网络，US 路由表必须包括有到该网络的静态路由。例如，如下图所示，ZXSEC US 设备必须配置到接口 192.168.10.1 与 192.168.10.2 的静态路由，为了将数据包分别转送到网络 1 与网络 2。

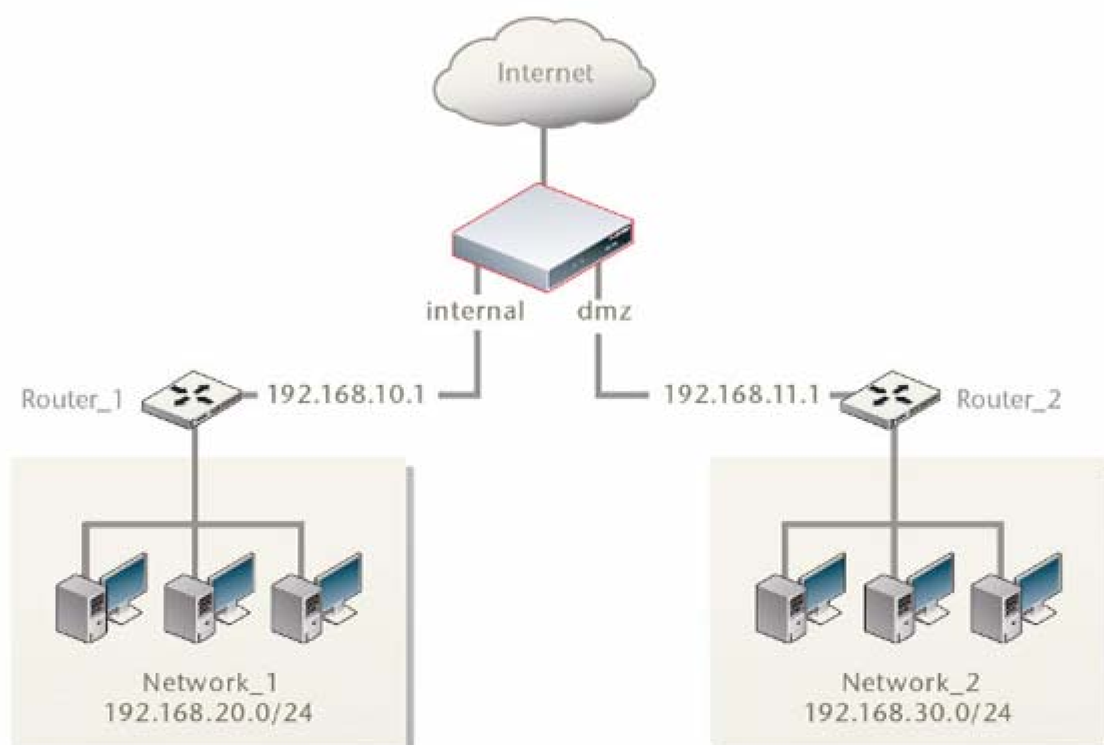


图10.3-3 目标地址在内部路由之后的网络

将数据包从网络 1 路由到网络 2，路由器 1 必须配置使用 ZXSEC US 内部接口（Internal）为默认的网关。在 ZXSEC US 设备上，您可以创建新的静态路由具有以下设置：

目标 IP/掩码：192.168.30.0/24

网关：192.168.11.1

设备：dmz

距离：10

将数据包从网络 1 路由到网络 2，路由器 1 必须配置使用 dmz 接口为默认的网关。在 ZXSEC US 设备中，您可以创建新的静态路由具有以下设置：

目标 IP/掩码：192.168.20.0/24

网关：192.168.10.1

设备：internal（内部）

距离：10

给默认的路由指定不同的网关默认的网关决定了与默认的路由相匹配的数据包将被转发到哪里。

给默认的路由指定不同的网关

1.　进入“路由>静态>静态路由表”。

2.　点击列表中第一行对应的编辑图标。

3.　在网关字段输入向外数据包流量指向的下一站中继路由的 IP 地址。

4.　如果 ZXSEC US 设备通过一个不同的接口与下一站路由器连接（相比较当前设备字段所选择的接口而言），从接口字段选择该接口的名称。

5.　在管理距离字段，可以调整管理距离的数值设置。

6.　点击 OK 确认。

在路由表中添加静态路由

路由中包含 ZXSEC US 设备将数据包转发到一个特殊目标地址的信息除了默认的网关以外，静态路由也可以将数据包转发到目标地址。

您可以手动定义静态的路由。静态路由控制 ForiGate 设备现有的数据流，您可以指定数据包通过哪个端口流出，以及到哪个设备进行分流。

进入路由>静态>静态路由，并点击“新建”添加静态路由条目。当您通过基于 web 的管理器添加静态路由时，ZXSEC US 设备将自动对新添加的静态路由设置一个次序编号并将路由添加在静态路由列表中。

下图所示的编辑静态路由的对话框属于 ZXSEC US 设备中接口名为“内部接口”的接口。在您配置的 ZXSEC US 设备中，接口名称有可以不同。

新建路由

目的 IP/掩码 0.0.0.0/0.0.0.0

设备 port2

网关 0.0.0.0

管理距离 10 (1-255)

OK 取消

图10.3-4 编辑静态路由

参数名称	参数说明
目的 **IP** 地址/掩码	输入该路由的目标 IP 地址与掩码默认路由的域值为 0.0.0.0/0.0.0.0。
网关	输入 ZXSEC US 设备将截取的数据包转发到的下一站路由的 IP 地址。设备 路由数据包通过的 ZXSEC US 接口名称。
管理距离	输入路由的管理距离。通过设定管理距离，您可以指定在具有相同目标地址情况下相对不同的路由具有优先权的路由.较低的管理距离是指相对更优先的路径。距离可以设置为 1 到 255 之间的任何整数。

10.4 策略路由

每当一个数据包到达 ZXSEC US 设备中任何一个接口时，ZXSEC US 设备将通过使用该数据包包头含代的源 IP 地址做逆向查询以识别该数据包是否在合法的接口接收的。如果 ZXSEC US 设备通过接受该数据包的接口不能与计算机的源 IP 地址通信，那么 ZXSEC US 将丢弃该数据包。

如果目标地址与本地地址能够匹配（并且本地配置允许数据包的传输），那么 ZXSEC US 设备将数据包传送到本地网络中如果数据包的传输目的地是其他的网络ZXSEC US 设备根据路由策略和/或存储在 ZXSEC US 转发路由表中的信息将把数据包转送在下一站中继路由（参见“有关路由”）。

当设置了路由策略并且数据包到达 ZXSEC US 设备时，ZXSEC US 设备根据策略路由表逐次查看并试图找到与该数据包相匹配的策略。如果发现匹配信息并且策略中包含了足够的信息路由数据包（必须注明下一站路由的 IP 地址以及将数据包转发 ZXSEC US 设备的接口），ZXSEC US 设备将使用策略中的信息路由数据包。如果没有与数据包相匹配的策略，ZXSEC US 设备将使用路由表路由数据包。

注意：因为大多数策略设置是可选项，一个匹配的策略可能还不足以提供给 ZXSEC US 设备足够的信息转发数据包。ZXSEC US 设备将转向参考路由表试图

将传送的数据包包头的信息与路由表中的路由相匹配。举例说明，如果策略中只列出向外的接口名称，ZXSEC US 设备将在路由表中查询下一站路由的 IP 地址。这种情况只有在 ZXSEC US 设备的接口是动态的接收 IP（例如对 ZXSEC US 设备接口设置了 DHCP 或 PPPoE）或因为 IP 地址是动态更改状态您不能够指定下一站路由的 IP 地址下发生。

进入路由>静态>策略路由，可以查看路由策略列表。在该项下。您还可以点击每条策略对应的编辑图标对现有的路由策略进行编辑。

下图所示的具有“外部接口”与“内部接口”的 ZXSEC US 设备中显示的策略路由。您所管理的 ZXSEC US 设备的接口名称可能不同。

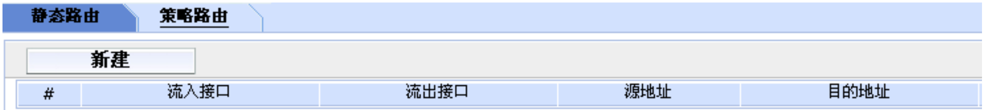


图10.4-1　策略路由列表

参数名称	参数说明
新建	添加新的策略路由。参见“添加路由策略”。
#	所配置路由策略的 ID 号.该号码是顺序排列的,除非策略项在列表中被移动改变位置。
流入接口	符合该策略路由的数据包在该接口被接收。
流出接口	数据包通过该接口进行路由。
源地址	策略路由将具有该源 IP 地址与掩码的数据包进行匹配。
目的地址	策略路由将具有该目标 IP 地址与掩码的数据包进行匹配。
删除与编辑图标	点击该图标删除活编辑策略路由。
移动图标	点击该图标可以在策略路由列表中移动策略路由条目。参见“移动策略路由”。

添加路由策略

路由策略选项是定义向内数据包的属性。如果一个数据包的属性与该策略所注明的条件相匹配，ZXSEC US 设备将通过指定的接口将数据包路由在指定的网关。

进入路由>静态>策略路由并点击“新建”可以添加路由选项。下图所示的具有“外部接口”与“内部接口”的 ZXSEC US 设备中显示的新策略路由的对话框。您所管理的 ZXSEC US 设备的接口名称可能不同。

新建策略路由

如果进入流量匹配:

协议端口 0

进入接口 loop1

源地址 / 掩码 0.0.0.0/0.0.0.0

目的地址 / 掩码 0.0.0.0/0.0.0.0

目的端口 从: 1 至: 65535

强制流量到:

流出接口

网关地址 0.0.0.0

OK 取消

图10.4-2 新路由策略

参数名称	参数说明
协议端口	根据数据包协议字段的数值执行策略路由，输入相匹配的协议号码该数值可以是 0 到 255 之间的任何数值设定为 0 将撤消该功能。
进入接口	点击选择接收流入数据包的接口。
源地址/掩码	根据数据包的 IP 源地址执行策略路由，输入相匹配的源地址与掩码。设定为 0.0.0.0./0.0.0.0 该撤消该功能。
目的地址/掩码	根据数据包的 IP 目的地址执行策略路由，输入相匹配的目的地址与掩码。设定为 0.0.0.0./0.0.0.0 该撤消该功能。
目的端口	根据接收数据包的接口执行策略路由。在"从"与"至"字段输入相同的端口号。如果您想将策略路由应用于一定范围的端口，设定起始与结束的端口号范围。设定为零表示撤消该功能项。
流出接口	输入路由数据包的接口名称。
网关地址	输入 ZXSEC US 设备可以功过指定接口访问的下一跳路由的 IP 地址。设定为 0.0.0.0 为无效 IP 地址。

移动路由策略

创建新的路由策略时，新的策略顺次添加在已有策略列表的末尾。如果您想设定一个策略优于其它策略，您可以将该策略移动在路由策略表的不同位置。

当两个策略项都是某一个数据包的匹配项时，例如 172.20.0.0./255.255.0.0.与 172.20.120.0/255.255.255.0。如果策略项中同时存在这两个策略，这两项策略同时与 172.20.120.112.相匹配，但是第二项更优越。这种情况下，最佳匹配的路由应该安插在策略路由表中其它路由项之前。

使用 CLI，您可以设定路由项的优先级别。在路由表中存在两项匹配的情况下，优先级的设置决定了使用哪一项路由。该功能只有使用 CLI 配置。

图10.4-3 移动策略路由

参数名称	参数说明
之前/之后	点击“之前”可以将所选的策略放在指定的策略之前。点击“之后”将所选的策略移动到指定的策略项之后。
策略路由 ID	选择输入某一路由项的 ID，您可以将所选的路由项移动至该 ID 路由项的之前或之后。

第11章 动态路由

11.1 概述

描述

本章就如何对路由流量配置动态路由协议通过大型或复杂的网络的内容进行了阐述。动态路由协议使得 ZXSEC US 设备自动与邻近的路由器共享信息，以及获得邻近路由器广播的路由与网络状态信息。ZXSEC US 设备支持以下的动态路由协议：

- 路由信息协议（RIP）
- 开放最短路径优先（OSPF）
- 边缘网关协议（BGP）



注意：

通过基于 web 的管理器可以配置基本的 RIP，OSPF 以及 BGP 路由选项。其它功能选项只能通过 CLI 命令配置。如何使用 CLI 命令配置 RIP，OSPF 以及 BGP 设置的详细信息，参见 ZXSEC US 设置 CLI 使用参考手册中“路由”章节。

根据您指定的规则，ZXSEC US 设备可以选择路由并动态更新路由表。给定一系列的规则，ZXSEC US 设备可以识别将数据包发送到目标地址的最佳路由或路径。您也可以定义规则禁止 ZXSEC US 设备向邻近的路由广播路由信息或更改在广播前更改路由信息。



注意：

ZXSEC US 设备在 root 虚拟域下运行 PIM（PIM: Protocol Independent Multicast）组播协议。ZXSEC US 设备支持 PIM 稀疏模式与密集模式并可以服务于与 ZXSEC US 设备接口连接的网段的多点传送服务器与接收器。PIM 可以使用静态路由、RIP、OSPF 或 BGP 将多点传送数据包转发到各自的目标地址。

双向转发（Bi-Directional Forwarding）是与 BGP 与 OSPF 协议协同工作的协议，能够快速检测到网络中不能被连接到的路由，且根据情况重新路由数据包直至路由恢复通畅。

内容

11.2 RIP（路由信息协议）

ZXSEC US 设备执行的 RIP（路由信息协议）既支持 RFC1058 定义的 RIP 版本 1 也支持 RFC2453 定义的 RIP 版本 2。RIP 版本 2 能够使 RIP 信息承载更多的信息并支持单一认证与子网掩码。



注意：

通过基于 web 的管理器可以配置基本的 RIP 选项。其它功能选项只能通过 CLI 命令配置。使用如何使用 CLI 命令配置 RIP，参见 ZXSEC US 设置 CLI 使用参考手册中“路由”章节。

RIP 是如何生效的

启动 RIP 后，ZXSEC US 设备从每个启动了 RIP 的接口广播 RIP 更新的请求。邻近的路由器将其路由表信息作为回应发送到 ZXSEC US 设备。ZXSEC US 设备将把从邻近路由获得的信息进行筛选，将设备路由表中不存在的路由信息添加在路由表中。当一条路由已经在路由表中存在,ZXSEC US 设备将广播的路由与记录在路由表中路由相比较筛选最佳路由。

RIP 是距离向量路由协议，适用于相对同构的网络。RIP 的度量是基于跳数的。跳数为 1 表示该网络直接与 ZXSEC US 设备相连接，跳数 16 表示 ZXSEC US 设备连接不到该网络。数据包到达目的地所穿越的每个网络通常规定为 1 跳。ZXSEC US 设备将两项到达同一目标地址的路由相比较，路由跳数较低的路由项将被添加到路由表中。

同样，当接口启动了 RIP 时，ZXSEC US 设备将以常规标准对邻近的路由器发送 RIP 响应。根据您对广播这些路由项的设置，更新信息中包含 ZXSEC US 设备路由的信息。您可以设定 ZXSEC US 发送更新的频率；一项路由在 ZXSEC US 路由表保持多长时间不被更新或不被定期更新；在一项路由从 ZXSEC US 路由表删除之前多长时间 ZXSEC US 设备广播该路由是不可达的。

查看并编辑 RIP 常规设置

配置 RIP 设置时，您必须指定运行 RIP 的网络以及与启动了 RIP 网络网络连接的 ZXSEC US 设备接口上需要调整 RIP 操作的其他选项。

进入路由>动态路由>RIP，配置与 RIP 网络连接的 ZXSEC US 设备的 RIP 常规选项。进入路由>动态路由>RIP，点击启动了 RIP 接口对应的编辑图标，可以编辑该接口的 RIP 操作参数。

下图所示的具有“外部接口”与“dmz 接口”的 ZXSEC US 设备中设置的常规 RIP 设置。您所管理的 ZXSEC US 设备的接口名称可能不同。

路由器ID 192.168.1.100 应用

高级选项(缺省, 重发布)

各个区 新建

区	类型	认证	
0.0.0.14	Regular	None	

各个网络 新建

网络	区	
192.168.1.24/255.255.255.248	0.0.0.14	

各个接口 新建

名称	接口	IP	认证	
port10	port10	192.168.1.28	None	

图11.2-1 RIP 常规设置

参数名称	参数说明
RIP 版本	点击选择 ZXSEC US 设备兼容的 RIP 版本您可以与启动了 RIP 设置的网络 连接的 ZXSEC US 设备所有接口的全局 RIP 设置。 ⌘ 选中 1 即发送与接收 RIP 版本 1 数据包。 ⌘ 选中 2 即发送与接收 RIP 版本 2 数据包。 ⌘ 选中“两者都”即表示发送与接收 RIP 版本 1 与版本 2 的数据包。如需要，您可以在具体的 ZXSEC US 接口取消全局设置。（参见“撤消接口的 RIP 操作参数”）
高级选项	点击打开设置 RIP 高级选项。参见“设置高级 RIP 选项”。
各个网络	与 ZXSEC US 设备连接的运行 RIP 的网络 IP 地址与掩码。当您将一个网络添加在网络列表中，与该网络连接的 ZXSEC US 设备的接口将在 RIP 更新中被广播。您可以对与 RIP 网络地址相匹配的 ZXSEC US 设备接口的 IP 地址启动 RIP 设置。 **IP**/掩码 输入启动了 RIP 设置网络的 IP 地址与掩码。 添加 点击将该网络的信息添加在网络列表中。
各个接口	ZXSEC US 设备接口中需要调整 RIP 操作的任何其他设置。 新建 击配置接口的 RIP 操作参数。这些参数将取代该接口设置全局 RIP 设置生效。参见“撤消接口的 RIP 操作参数”。 接口 点击选择配置 RIP 参数的接口。 发送 选择通过每个接口发送更新的 RIP 版本。 接收 选择每个接口中用户获得更新的 RIP 版本号。 认证 选择该接口的认证类型：无，文本或 MD5。 被动 点击设置在该接口屏蔽 RIP 广播。
删除与编辑图标	删除或编辑一项 RIP 网络条目或 RIP 接口定义。

设置高级 RIP 选项

高级 RIP 选项设置中，您可以设定 RIP 计时以及定义重新分配路由的跳数，重新分配路由的信息可以是 ZXSEC US 设备通过除了 RIP 更新的其他方法获得的。例如，如果 ZXSEC US 设备与一个 OSPF 或 BGP 网络连接，或者您在 ZXSEC US 路由表中手动添加了静态路由，您可以配置通过启动了 RIP 设置的接口广播这些路由信息。

进入路由>动态路由>RIP 项下，可以点击设置高级 RIP 选项。选项设置完成后，点击“应用”生效。



注意：

通过 CLI 可以配置其它的 RIP 高级选项。例如，您可以路由图或访问列表以及前缀列表过滤向内与向外的路由更新。ZXSEC US 设备也支持偏移值列表，指定的偏移量设置值将被添加在路由的跳数中。

路由器ID 192.168.1.100 应用
高级选项(缺省，重发布)
缺省信息 无 经常 总是
重发布
连接的 RIP
距离 10 (1-16777214) 距离 10 (1-16777214)
静态 BGP
距离 10 (1-16777214) 距离 10 (1-16777214)

图11.2-2 高级选项（RIP）

参数名称	参数说明
缺省跳数	输入 ZXSEC US 应该分配到添加在路由表中的跳数跳数设置的范围是 1 到 16 之间任何的数字。除非另行指定，该值同样适用于路由重新发布设置。
启动产生缺省路由	点击生成并无条件将路由信息广播到与 ZXSEC US 设备相连接的启动 RIP 设置的网络。所生成的路由信息可以是基于动态路由协议或路由表中的路由信息。
RIP 定时器	替换默认的 RIP 计时器设置。默认的设置对于大部分配置是可以生效的您更改这些设置时请确定新的设置与本地路由器火访问服务器是可以兼容的。
更新	RIP 更新发送的时间间隔（秒计）。
失效	将失效的路由信息删除之前的计时。如果 RIP 在超时计时器之后但是在 Garbage 计时器超时之前接收到一个路由更新，该更新将是有效的。
超时	一条路由信息宣布无效之后时间间隔(以秒计)。该路由信息将从路由表中删除。RIP 保持该路由直至 garbage 计时超时，然后将该路由删除。如果在超时计时器过时之前 RIP 接收到一条更新，超时计时器将重新启动计时。如果 RIP 在超时计时器过时之后但是在 garbage 计时器过期之前接收到一条路由更新，该更新将恢复为可以获得的信息超时计时器的设置值应该是更新计时器设置值的至少三倍。
路由重发布	启动或撤消通过 RIP 获得路由的 RIP 更新。ZXSEC US 设备可以使用 RIP 将直接连接的网络，静态路由，OSPF 或 BGP 获得的路由信息重新发布。

直连路由	广播从直接连接的网络获得的路径。如果您设定这些路由的跳数，可以在跳数字段输入跳数值。该值的设定范围是 1 到 16 之间的任何整数。
静态路由	广播从静态路由获得的路由信息。如果您设定这些路由的跳数，可以在跳数字段输入跳数值。该值的设定范围是 1 到 16 之间的任何整数。
OSPF	广播从 OSPF 获得的路由信息。如果您设定这些路由的跳数，可以在跳数字段输入跳数值。该值的设定范围是 1 到 16 之间的任何整数。
BGP	广播从 BGP 获得的路由信息。如果您设定这些路由的跳数，可以在跳数字段输入跳数值。该值的设定范围是 1 到 16 之间的任何整数。

替换接口中的 RIP 操作参数

通过 RIP 接口选项您可以中止应用于与启动了 RIP 设置网络连接的全部 ZXSEC US 接口的全局 RIP 设置。例如，如果您想中止一个与启动了 RIP 设置网络的子网连接接口的 RIP 广播，您可以设置接口以被动模式操作。被动模式下的接口只接收 RIP 更新但对 RIP 请求不做出回应。

如果接口启动了 RIP 版本 2，您可以设置密码验证确保 ZXSEC US 设备从路由器接收更新之前对邻近的路由器进行验证 ZXSEC US 设备与邻近的路由器必须配置了相同的密码。验证设置保证了更新数据包的真实性，但并不验证数据中路由信息的机密性。

进入路由>动态路由>RIP，并点击“新建”可以对启动了 RIP 设置的接口设置具体的 RIP 操作参数。



注意：

其它设置选项如水平分割与密钥串设置可以通过 CLI 对每个接口进行设置。详细信息参见 ZXSEC US 设备 CLI 使用参考手册中“路由”章节中的叙述。

下图所示是具有接口名称为“内部”接口的 ZXSEC US 设备中新建/编辑 RIP 接口的对话框。您所管理的 ZXSEC US 设备接口的名称可能与图例中所示的接口名称不同。

新建/编辑RIP接口

接口 loop1

发送版本 ◉1 ○2 ○两者都支持

接收版本 ◉1 ○2 ○两者都支持

认证 None

被动接口 ☐

OK 取消

图11.2-3 新建/编辑 RIP 接口

参数名称	参数说明
接口	选择这些设置适用的 ZXSEC US 接口的名称。该接口必须与启动了 RIP 配置的网络连接。该接口可以是虚拟 IPSec 或 GRE 接口。
发送版本/接收版本	为通过接口发送与接收更新设置默认的兼容 RIP：RIP 版本 1，RIP 版本 2 或两者都。
认证	选择在指定的接口发送与接收的 RIP 信息验证的方式。 ● 如果您将验证设置为“无”，将不执行验证。 ● 如果接口与运行 RIP 版本 2 的网络连接，可以选择“文本”方式验证并在密码字段中设置密码（密码最大可以设置为 35 个字符）。ZXSEC US 设备与 RIP 更新路由器必须配置相同的密码。密码通过网络以文本格式发送。 ● 选择 MD5 即使用 MD5 验证来往的 RIP 更新。
被动接口	设置接口不广播路由信息。如要接口对 RIP 请求作出反应，撤消该设置。

11.3 OSPF

OSPF(OSPF: open shortest path first)是一种链路状态协议，最常用于异构网络中在相同的自主域(AS: automonous system)中共享路由信息。ZXSEC US 设备支持 OSPF 版本 2（参见 RFC2328）。



注意：

通过基于 web 的管理器可以配置基本的 OSPF 路由选项。其他选项只有通过 CLI 命令配置。有关使用 CLI 命令配置 OSPF 设置的详细信息，参见 ZXSEC US 设备 CLI 使用参考手册中“路由”章节。

OSPF 自主域

一个 OSPF 自主域(AS: automonous system)是由边界路由器链接的分割为不同的逻辑区域组成的系统。一个区域由一组同构网络构成。一个区域边界路由器通过一个或多个区域链接到 OSPF 主干网络（区域 ID 为 0）。有关定义 OSPF 自主域的特点，参见"定义 OSPF 自主域"。

当 ZXSEC US 设备的接口连接到 OSPF 区域时，便可以参与 OSPF 通信。ZXSEC US 设备使用 OSPF Hello 协议获取区域中邻接路由信息。路由邻接是指任何与 ZXSEC US 设备共同连接到同一区域的路由接口。初始接洽完成后，ZXSEC US 设备将与其 OSPF 邻接规律地交换 Hello 数据包用来确定邻接的路由是否可达。

每当邻接路由的状态更改时或新的路由邻接上线时，运行 OSPF 协议的路由器生成链接状态通告并将该报告发送到邻接的路由。只要 OSPF 网络是稳定的，OSPF 邻接路由之间的链路状态通告将保持不变。链路状态通告(LSA: Link-State Advertisement)识别一个区域中所有运行 OSPF 协议的路由器的接口并提供有关信息使运行 OSPF 协议的路由器选择到达目的地址的最短路径。运行 OSPF 协议的路由器之间所有的链路状态通告都是设置进行验证的。

ZXSEC US 设备根据从运行 OSPF 协议的路由器接收到的通告组成并维护一个链路状态信息数据库。ZXSEC US 设备将对保存的链路状态信息应用最短路径优先（SPF）算法以便算出到目标地址的最优（最短）路径。OSPF 利用量度（cost）计算最短路径。一条路由的量度是通过将与外向接口发生通信的到达目的路径进行量度累加计算出来的。总体量度最低的也就是最佳路由。

ZXSEC US 设备根据 SPF 的计算结果动态更新其路由表以确保 OSPF 数据包使用最短路径路由到其目的地。根据网络的拓扑，ZXSEC US 路由表中的条目可以包括：

- 本地 OSPF 区域中的网络地址（到达该网络的数据包直接被发送）。
- 到 OSPF 区域边界路由器的路由（路由到其它区域的数据包）。
- 如果网络包含 OSPF 区域与非 OSPF 区域，路由到自主域(AS)边界路由器，该路由器存在于 OSPF 主干网络并配置用来将数据包转发到 OSPF 自主域以外的目标地址。

ZXSEC US 设备通过 OSPF 可以获知的路由数量取决于网络的拓扑结构。如果 OSPF

网络配置得当，一台 ZXSEC US 设备能够支持一万条路由。

定义 OSPF 自主域

定义 OSPF 自主域，包括：

- 定义一个或多个 OSPF 区域特征。
- 建立所定义的区域与属于 OSPF 自主域的本地网络的通信连接。
- 如需要，调整启动了 OSPF 设置的接口配置。

有关如何使用基于 web 管理器执行以上任务的详细信息，参见以下步骤。

定义 **OSPF** 自主域

1. 进入路由>动态路由>OSPF。
2. 在“区域”项下，点击“新建”。
3. 定义一个或多个 OSPF 区域特征。参见“定义 OSPF 区域”。
4. 在“网络”项下，点击“新建”。
5. 建立所定义的区域与属于 OSPF 自主域的本地网络的通信连接。参见“设定 OSPF 网络”。
6. 如需要，调整启动了 OSPF 设置的接口配置。点击“接口”项下的“新建”。
7. 配置接口的 OSPF 操作参数。参见“配置 OSPF 接口的操作参数”。
8. 如需要，配置其他启动了 OSPF 设置接口的参数。
9. 如需要，点击配置 OSPF 自主域的“高级 OSPF 选项”。参见“设置高级 OSPF 选项”。
10. 点击“应用”。

查看与编辑基本的 OSPF 设置

当您配置 OSPF 设置时，您需要定义自主域运行 OSPF 以及指定 ZXSEC US 设备中哪个接口与自主域连接。作为定义自主域的一部份，您必须设定自主域并设定哪个网络包含这些区域。您也可以调整设置运行 OSPF 的 ZXSEC US 设备接口设置。

进入路由>动态路由>OSPF，查看并编辑 OSPF 设置。

路由器ID 192.168.1.100 应用

▶ 高级选项(缺省，重发布)

各个区 新建

区	类型	认证	
0.0.0.14	Regular	None	

各个网络 新建

网络	区	
192.168.1.24/255.255.255.248	0.0.0.14	

各个接口 新建

名称	接口	IP	认证	
port10	port10	192.168.1.28	None	

图11.3-1 基本的 OSPF 设置

参数名称	参数说明
路由 ID	输入唯一性的路由 ID,用以识别将 ZXSEC US 设备与其它 OSPF 路由加以区分。常规情况下，该路由 ID 是 OSPF 自主域中按序分配到 ZXSEC US 任何一个接口的最高 IP 地址。OSPF 运行时请不要衣更改路由 ID。
高级选项区	设置高级 OSPF 选项。参见“设置高级 OSPF 选项”。 有关组成 OSPF 自主系统的区域的信息。OSPF 数据包的包头包含一个区域 ID，该 ID 用来识别自主系统中的数据包发生源。 创建　点击定义一个 OSPF 区域并将该区域添加到区域列表中。参见“定义 OSPF 区域”。 区域　区域 ID 为 0.0.0.0.是自主系统的主干区域，不能够更改或删除。
类型	自主系统中区域的类型。 ⌘ 如果有关区域是一个常规的 OSPF 区域，该字段显示“常规”。 ⌘ 如果该区域是非纯末梢区域，显示“NSSA”。 ⌘ 如果该区域是 stub 区域，显示“Stub”。 详细信息，参见“定义 OSPF 区域”。
验证	通过与每个区域链接的所有 ZXSEC US 接口发送与接收 OSPF 数据包的验证方法。 ⌘ 没有启动验证设置时显示“无”。 ⌘ 启动基于文本的密码验证时显示“文本”。 ⌘ 启动 MD5 验证时显示“MD5”。 在一个区域中的一些接口可以应用不同的验证设置，不同的验证方法将在接口的设置项下显示。例如，如果一个区域只应用密码验证，您可以在该区域中的一个或多个网络的中设置不同的密码。

各个网络	OSPF 自主系统中的网络与其区域 ID。将网络添加在网络列表中，与该网络发生通信的全部接口的信息将全部列入 OSPF 链路状态通告。您可以对 IP 地址与 OSPF 网络地址相匹配的接口启动 OSPF 设置。 新建 点击在自主系统中添加网络以及设定该区域的 ID，并将新建的网络添加在网络列表中。参见“设定 OSPF 网络”。 网络 自主系统中运行 OSPF 网络的 IP 地址与掩码。设备中可能有物理接口或 VLAN 接口与该网络连接。 区域 分配到一个 OSPF 网络的 ID。
各个接口	设备接口中 OSPF 设置的其他选项。 新建 点击对设备接口添加其它的 OSPF 操作参数，并将新建接口添加到接口列表中。参见“设置 OSPF 接口的 操作参数”。 名称 OSPF 接口的名称。 接口 配置了 OSPF 设置的设备物理或 VLAN 接口名称，用于区分在同一区域中分配到其它接口的默认值。 IP 具有其它的不同设置的启动了 OSPF 配置接口的 IP 地址。 验证 验证通过启动了 OSPF 设置的接口发送与接收链路状态通告的方法。该设置将代替区域验证的设置。
删除与编辑图标	点击删除或编辑 OSPF 区域条目，网络条目或接口定义项。

设置高级 OSPF 选项

高级 OSPF 选项中，您可以指定重新分布路由的跳数，该跳数是 ZXSEC US 设备除了从 OSPF 链路状态通告之外通过其它方法获得的。例如，如果 ZXSEC US 设备与一个 RIP 或 BGP 网络连接，或您手动在 ZXSEC US 路由表中添加了静态路由；您可以配置 ZXSEC US 设备向启动了 OSPF 设置的接口广播这些路由信息。

进入路由>动态路由>RIP，可以扩展 RIP 选项设置高级 RIP 选项。设置完成后，点击“应用”生效。

图11.3-2 高级选项（OSPF）

参数名称	参数说明
缺省信息	生成并将缺省的（外部）路由广播到 OSPF 自主域。路由是根据动态路由协议或路由表中的路由生成的。 无　中止生成缺省路由。 经常 只要 ZXSEC US 设备路由表中存储有路由信息便在 OSPF 自主域中生成缺省路由并将路由信息广播至邻接的自主域。 总是 无条件在 OSPF 自主域中生成缺省路由并将路由信息广播至邻接的自主域，即使 ZXSEC US 设备路由表中没有存储的路由信息。
重新分布	启动或中止 OSPF 链路状态通告那些并非从 OSPF 获得的路由信息。ZXSEC US 设备可以使用 OSPF 重新分布从直接连接的网络，静态路由，RIP 和/或 BGP 获得的路由。 连接的 点击重新分布直接从相连接的网络获得的路由。如果您想设定这些路由的量度，在量度字段输入 1 到 16777214 之间的数值。 静态　点击重新分布从静态路由信息获得的路由。如果您想设定这些路由的量度，在量度字段输入 1 到 16777214 之间的数值。 **RIP**　点击重新分布从 RIP 获得的路由。如果您想设定这些路由的量度，在量度字段输入 1 到 16777214 之间的数值。 **BGP**　点击重新分布从 BGP 获得的路由。如果您想设定这些路由的量度，在量度字段输入 1 到 16777214 之间的数值。



注意：

其它还有很多高级 OSPF 选项是通过 CLI 进行配置的。有关配置的详细信息，参见 ZXSEC US 设备 CLI 使用参考手册中“路由”章节叙述。

定义 OSPF 区域

一个区域逻辑上定义为 OSPF 自主域中的一部分。每个区域均是 32 比特以十进制逗点分隔的区域 ID 加以区别。ID 为 0.0.0.0 是 OSPF 网络的主干区域。您可以将其余的区域划分为以下任何一种类型：

标准区域（Regular）

Stub

NSSA

一个标准区域包含不止一个路由器，每个路由器都至少具有一个启动了 OSPF 设置的接口与区域连接。

为了到达 OSPF 主干区域，stub 区域中的路由器必须发送数据包到区域边界路由器去向非 OSPF 域的路由将不在 stub 区域中广而告之区域边界路由器只向 OSPF

自主域广播一条默认的路由（目标地址为 0.0.0.0.）并存入 stub 区域，这样确保了任何不能与具体的路由相匹配的数据包能够与默认的路由匹配。与 stub 区域连接的任何路由都是该区域的一部分。

NSSA(NSSA: Not-So-Stubby Area)区域中超出区域之外路由到非 OSPF 域的路由将会报知 OSPF 自主域。但是，该区域本身仍然被其它的自主域当作为一个 stub 区域。

标准区域以及 stub 区域（包括 NSSA 区域）通过区域边界路由器与 OSPF 主干区域相连接。

进入“路由>动态路由>OSPF”，在“区域”项下点击“新建”可以定义 OSPF 区域。同样在该菜单下，点击一个区域对应的编辑图标可以编辑 OSPF 区域的属性。



注意：

如需要，您可以定义一条到某一区域的虚拟链接，该链接不存在到 OSPF 主干区域的物理连接虚拟链接只有当 ZXSEC US 设备作为区域边界路由器的时候在设备之间建立。有关建立虚拟链接的详细信息，参见 ZXSEC US 设备 CLI 使用参考手册中 OSPF 配置命令“config area”的子命令“config virtual-link”的使用。

新建/编辑OSPF区

区 (IP)

类型 Regular

认证 None

OK 取消

图11.3-3 新建/编辑 OSPF 区

参数名称	参数说明
区域	输入区域 ID该数值必须类似一个 IP 地址的格式以逗点分隔的十进制位值。 OSPF 区域创建后，该区域的 ID 将不能更改。

类型	点击选择分配到区域中的网络类型。 ● 如果区域中包含不止一个路由器，而且每个路由器至少有一个启动了 OSPF 配置的接口与区域连接；那么点击“regular”。 ● 如果超出区域之外路由到非 OSPF 域的路由将会报知 OSPF 自主域。但是该区域本身仍然被其它的自主域当作为一个 stub 区域点击“NSSA”。 ● 如果区域中的路由器必须发送数据包到一个区域边界路由器以便到达主干区域,同时您不想到非 OSPF 域的路由在区域中的路由器范围内广播；点击“Stub”。
验证	选择区域中通过所有接口发送与接收 OSPF 数据包验证的方式。 ● 设置为“无”中止验证设置。 ● 设置为“文本”启动基于文本的密码验证方式使用纯文本的密码验证来往的链路状态通告。 ● 设置为“MD5”，使用 MD5 hash 验证。 如需要，您可以在区域的接口设置不同的验证方式，在接口设置的验证方式优先于该设置。

注意：

有关对区域分配网络的信息，参见“设定 OSPF 网络”。

设定 OSPF 网络

OSPF 区域由多个邻接的网络共同构成。当您对网络分配区域 ID 时，该区域的属性同时适用该网络。

进入路由>动态路由>OSPF 并在“网络”菜单项下点击“新建”，对网络分配 OSPF 区域 ID。同样在 OSPF 项下，点击每项网络对应的编辑图标可以更改分配到该网络的区域 ID。

新建/编辑OSPF网络	
IP/掩码	192.168.1.24/255.255.255.248
区域	0.0.0.14
OK	取消

图11.3-4 新建/编辑 OSPF 网络

参数名称	参数说明
IP/掩码	输入所要分配区域 ID 的本地网络的 IP 地址与掩码。
区域	给网络分配区域 ID区域的属性设置必须与指定网络的属性与网络拓扑结构相符。在选择区域 ID 之前，先要定义一个区域。参见“定义 OSPF 区域”。

设定 OSPF 接口的操作参数

OSPF 接口定义是指对启动了 OSPF 设置的 ZXSEC US 设备的接口设定具体的操作参数。定义接口包括定义接口的名称（例如，外部接口或 VLAN_1），对接口分配 IP 地址，以及设置通过该接口进行链路状态通告（LSA）互换时验证的方式，接收与发送 OSPF Hello 报文的计时与 dead-interval 数据包。

您可以对所有 ZXSEC US 接口中 IP 地址与启动了 OSPF 设置的网络相匹配的接口启动 OSPF 设置。例如所定义的区域 ID 为 0.0.0.0.而且 OSPF 网络定义为 10.0.0.0/16；然后将 vlan1 定义为 10.0.1.1/24，vlan2 为 10.0.2.1/24 以及 vlan3 为 10.0.3.1/24。这三个 vlan 都应用于区域为 0.0.0.0 运行 OSPF 设置。启动这些接口，您可以创建 OSPF 网络能够与具体的 IP 地址相匹配的一个区域。

当相同的 ZXSEC US 接口被分配了不止一个 IP 地址时，您可以对该接口配置不同的 OSPF 操作参数。例如，相同的 ZXSEC US 接口可以通过不同的子网连接到两个成为邻居的路由器。您可以配置一个 ODPF 接口的定义包括与一个邻居路由器相兼容的 hello 报文与 dead-interval 参数，设置同一个接口的第二个 OSPF 定义与第二个邻居路由的设置相兼容的参数。

进入路由>动态路由>OSPF，在“接口”菜单项下点击“新建”可以设置接口的 OSPF 操作参数。点击接口对应的编辑图标，可以编辑接口的 OSPF 操作参数。

新建/编辑OSPF接口

名称

接口 loop1

IP 0.0.0.0

认证 None

计时(秒)

Hello间隔 10 (1 - 65535)

Dead间隔 40 (1 - 65535)

OK 取消

图11.3-5 新建/编辑 OSPF 接口

参数名称	参数说明
名称	输入 OSPF 接口的名称例如,该名称可以包含说明接口与哪个 OSPF 区域相链接。
接口	选择与该 OSPF 接口相通信的 ZXSEC US 设备的接口。例如，port1,external 接口或 VLAN_1。ZXSEC US 设备可以使用物理接口，VLAN，虚拟 IPSec 或 GRE 接口连接启动了 OSPF 设置的网络。
IP 地址	输入分配到启动了 OSPF 设置接口的 IP 地址。该接口将支持运行 OSPF，因为其 IP 地址与 OSPF 网络的地址相匹配。 例如，如果您定义 OSPF 网络地址为 170.20.120.0/24,对 port1 分配的 IP 地址为 172.20.120.140 与网络地址相匹配，那么该接口启动了 OSPF 设置。
认证	设置在指定接口 LSA 互换时的验证方式。 ⌘ 设置为“无”中止验证。 ⌘ 设置为“文本”即使用基于存文本的密码方式验证 LSA密码的设置最大长度为 35 个字符。 ⌘ 设置为“MD5”使用一个或更多密钥生成 MD5 hash。 该设置优先于区域中设置的验证设置。
密码	输入纯文本格式的密码。输入一串字母数字混合的最多为 15 位的字符。发送 LSA 到该 ZXSEC US 接口的 OSPF 邻居必须配置使用相同的密码。密码输入字段只有您使用以纯文本密码方式验证时可用。

MD5 密钥	在 ID 字段（范围为 1 到 255），对（第一个）密码输入密钥标识符。然后在密钥字段输入相关的密码。该密码的最大设置长度是 16 位数字与字母混合的字符串。发送 LSA 到该接口的 OSPF 邻居必须设置相同的 MD5 密钥。如果 OSPF 邻居使用不止一个密钥生成 MD5 hash，点击添加图标将其它的 MD5 密钥添加在列表中该字段只有您设置以 MD5 方式验证时可用。
Hello 间隔	作为可选项，设置 hello interval 与所有 OSPF 邻居的 Hello interval 设置相兼容。该时间间隔是通过该接口等待发送 hello 数据包的时间。
失效间隔	作为可选项，置失效间隔与所有 OSPF 邻居的失效间隔设置相兼容。该设置是定义是 ZXSEC US 设备等待通过接口从 OSPF 邻居接收 hello 数据包的时间间隔。如果 ZXSEC US 设备没有在设定的时间内接收 hello 数据包，ZXSEC US 设备将认为该 OSPF 邻居不可达。常规配置下，失效间隔的设置值要是 hello 间隔设置值的四倍。

11.4 BGP

BGP 是 ISP 用来在不同的 ISP 网络之间交换路由信息的互联网路由协议。例如，BGP 可以在自主域中通过使用 RIP 和/或 OSPF 实现共享 ISP 网络之间的路径。ZXSEC US 设备的 BGP 实现支持 BGP-4 并与 RFC-1771 兼容。

BGP 是如何生效的

启动 BGP 设置后，每当 ZXSEC US 设备路由表中任何一部分更改时，ZXSEC US 设备将发送路由表更新到邻接的自主域(AS)。每个自主域，包括 ZXSEC US 设备所属的本地自主域都配置了自主域编号。自主域编号将参考特殊目标网络。

BGP 更新同时将最佳路径广播到目标网络。当 ZXSEC US 设备接收到 BGP 更新，ZXSEC US 设备将可能的路由的多口标识(MED)进行核对以便将路径记录在 ZXSEC US 路由表之前识别到达目标网络的最佳路径。

BGP 设置有时会重新启动。当路由故障设置允许转发时，BGP 重新启动将影响转发的功效。



注意：

通过基于 web 的管理器可以配置基本的 BGP 路由选项。其它配置选项只有通过 CLI 配置。有关使用 CLI 配置 BGP 的详细信息，参见 ZXSEC US 设备 CLI 使用手册中“路由”章节。

查看与编辑 BGP 设置

配置 BGP 时,设定包含 ZXSEC US 设备在内的自主域并对 ZXSEC US 设备设置一个路由器 ID 以区别其它 BGP 路由器。您也必须明确 ZXSEC US 设备的邻居并指定 ZXSEC US 设备所属的哪个网络信息应该广播到 BGP 邻居。

进入路由>动态路由>BGP，查看并编辑 BGP 设置。通过基于 web 的管理器可以进行基本的 BGP 配置。其它配置选项只有通过 CLI 配置。有关使用 CLI 配置 BGP 的详细信息，参见 ZXSEC US 设备 CLI 使用手册中"路由"章节。

图11.4-1 基本的 **BGP** 选项

参数名称	参数说明
本地自主域	输入 ZXSEC US 设备所属的本地自主域的编号。
路由 ID	输入 ZXSEC US 设备唯一性的路由 ID 以区别于其他 BGP 路由器。路由 ID 是十进制格式的以逗点分隔的 IP 地址如果您在 BGP 运行时更改路由 ID，所有到 BGP 对等的连接都将暂时中止直到重新建立连接。
多个邻居	邻接自主域中 BGP 对等体的 IP 地址与自主域编号。 **IP** 输入连接到 BGP 网络的邻居接口的 IP 地址。 远程自主域 输入邻居所属的自主域的编号。 添加/编辑 点击将网络信息添加到网络列表中。 网络 被广播到 BGP 对等的网络 IP 地址与掩码。
多个网络	输入对 BGP 队等体广播的 IP 地址与网络掩码。ZXSEC US 设备的物理接口或 VLAN 接口与这些网络存在连接。 **IP/**掩码 被广播的网络的 IP 地址与掩码。 添加 点击"添加"在网络列表中添加网络信息。 网络 被广播到 BGP 队等体的主要网络的 IP 地址与掩码。 删除图标 点击删除一个 BGP 邻居条目或 BGP 网络。

组播

ZXSEC US 设备可以作为 root 虚拟域中独立组播协议（PIM）版本 2 路由器，ZXSEC US 设备支持 PIM 稀疏模式（RFC2362）与 PIM 密集模式（RFC 3973）以及为网段中与 ZXSEC US 设备接口连接的组播服务器或接收器提供服务。

组播服务器程序使用一个（Class ID）组播地址将一个数据包的备份发送到一组接收器中。网络中的 PIM 路由确保只有数据包的一个备份通过网络转发直到传送到终点目的地。在终点目的地，因为客户端程序发出请求将数据包流量发送到组播地址，数据包只有在被要求将信息传送到多点客户端程序时需要被复制。



注意：

发送/接收程序以及 PIM 路由器之间的连接必须都配置使用 PIM 版本 2 才能够支持 PIM 通信。PIM 可以使用静态路由、RIP、OSPF、或 BPG 将组播数据包转发到其目的地址。启动源到目的地址数据包的发送，需要在所有 PIM 路由器接口启动稀疏模式或密集模式。运行于稀疏模式的路由器不能发送组播信息到运行于密集模式的路由器。另外，如果一台 ZXSEC US 设备处于一个源与 PIM 路由器之间，或直接与一个接收器连接，您必须手动创建防火墙策略允许在源与目标地址之间通过组播数据包或封装数据包（IP 流量）。

PIM 是由多个邻接的网络组成的一个逻辑上的区域。该区域包括至少一个 BSP（Boot Strap Router）。如果启动运行于稀疏模式，PIM 域中还包含许多汇集点（Rendezvous Points）与指定的路由器（Designated Routers）。当启动 ZXSEC US 设备的 PIM 设置时，ZXSEC US 设备可以配置的任何时间内执行这些功能。如果需要运行于稀疏模式，您可以定义静态汇集点（RPs）。



注意：

通过基于 web 的管理器可以配置基本的选项。其它配置选项只有通过 CLI 配置。有关使用 CLI 配置 PIM 的详细信息，参见 ZXSEC US 设备 CLI 使用手册中“组播”章节。

查看与编辑组播设置

启动组播（PIM）路由设置后，您可以在接口配置运行稀疏模式或密集模式。进入路由>动态路由>多播路由，可以查看并编辑 PIM 设置。通过基于 web 的管理器

可以配置基本的 PIM 设置。其他高级 PIM 选项可以通过 CLI 配置。详细信息参见 ZXSEC US 设备 CLI 使用参考手册中“路由”章节。

启动多播路由
静态集合点(RPs) RP地址
应用
新建

接口	模式	RP候选者		DR优先级	
		状态	优先级		

图11.4-2 基本组播选项

参数名称	参数说明
启动多播路由	选中该功能框启动 PIM 版本 2 路由。您必须在源与目标地址之间启动了 PIM 设置的接口创建防火墙策略允许通过封装与未封装的数据包。
添加静态 **RP**	如有运行于稀疏模式的需要，输入 RP（汇集点）的 IP 地址，该汇集点可以作为一个组播组的数据包分布树。组播组发送连接信息（Join messages）到 RP，从源地址发送的数据将被传送到 RP。 如果一个指定 IP 的组播组的 RP 对于 BSR 是已知的，那么该已知的 RP 将被使用，您指定的静态 RP 地址将被忽略。
应用	点击“应用”保存设定的静态 RP 地址。
新建	点击创建接口新的组播条目。该设置可以使您在指定的接口调整 PIM 操作或在特殊的接口设置 PIM 设置优先于全局 PIM 设置生效。参见“在接口设置优先执行的组播设置”。
接口	进行 PIM 设置的接口名称。
模式	接口运行的 PIM 操作模式（稀疏模式或密集模式）。
状态	接口的稀疏模式下 RP 候选的状态。点击接口对应的编辑图标可以启动或中止接口的 RP 候选设置。
优先级	该接口 RP 候选的优先级设置。该设置只有在启动了 RP 候选时可用。
DR 候选者	对接口分配的指定路由器（Designed Router）候选的优先级别设置。该设置只有在稀疏模式下可用。
删除与编辑图标	点击删除或编辑接口的 PIM 设置。

在接口设置优先执行的组播设置

通过接口的 PIM 设置选项，您可以对与 PIM 域连接的 ZXSEC US 的接口设置 PIM 操作参数。例如，您可以对于启动了 PIM 网段连接的接口启动运行密集模式。启

动稀疏模式后，您可以调整接口用于广播汇集点（RP）和/或指定的路由器（Designated Router）候选的优先级设置。

新建

接口	loop1
PIM模式	松散模式
DR优先级	1 (1 - 4294967295)
RP侯选者	
RP侯选者优先级	1 (1-255)

OK 取消

图11.4-3 组播接口设置

参数名称	参数说明
接口	点击选择应用这些设置 ZXSEC US 的 root 虚拟域接口的名称。该接口必 须与启动了 PIM 版本 2 设备的网段连接。
PIM 模式	选择操作模式：稀疏模式或密集模式。所有与统一网段连接的 PIM 路由器必须运行于同一种模式。如您选择了稀疏模式，需要设置以下选项。
DR 优先级	设置 ZXSEC US 接口广播 DR 候选的优先级别。设置范围为 1 到 4294967295。该设置值将与同一网段的其他所有 PIM 路由器的 DR 比较，具有最高 DR 优先级设置值的路由将被选作 DR。
RP 候选者	启动或中止接口的 RP 候选设置。
RP 候选者优先级	输入接口的 RP 候选优先级设置。设置范围是 1 到 255 之间的数值。

多播目标 NAT

多播目标 NAT（DNAT）允许您将外部所接收的多播目标地址转换为与机构内部寻址策略相符合的地址。

应用该功能，用户不需要在转换边界重新分布路由与符合自己的网络架构以便反向传输路径转发（RPF: reverse path forwarding）能够正常工作，且用户可以从网络中的两个 Ingress 点接收相同的流量然后独立的对其配置路由。

进入 CLI，使用以下命令配置多播 DNAT：

```
config firewall

multicast-policy edit pl

set dnat <dnatted-multicast-group>
```

set …..

next

end

详细信息，参见 ZXSEC US 设备 CLI 使用操作手册中的防火墙（firewall）章节。

11.5 双向转发检测(BFD)

双向转发检测(BFD: Bi-directional Forwarding Detection)协议设计用于处理动态路由协议的不足，对于网络中设备的故障不能具有很细密的检测力度以及围绕这些故障进行的重新路由。BFP 能够以毫秒计时检测到这些故障，之前路由协议只能够以秒检测这些故障且得花费较长的时间对这些故障做出反应。

ZXSEC US 设备支持 BFD 应用，作为 OSPF 与 BGP 的一部分。BFD 只能通过 CLI 进行配置。

BFD 是如何生效的

ZXSEC US 设备中启动 BFD 后，BFD 将试图连接到网络中的其他路由器。您可以通过在一个接口启动 BFD 来限制 BFD 查询以及在网络中对具体的邻居路由器启动 BFD。

BFD 建立与路由器的连接后,BFD 将继续定期发送数据包到路由器,以确定路由器是否运行。这些小数据包发送比较频繁。

如果 BFD 没有连接到网络中的路由器便不能报告路由器是否工作。这种情况下，BFD 将继续试图连接到路由器。直至建立连接，设备在没有通知的情况下可能运行或关闭。

在设定的时间段内，没有得到来自邻居路由器的回应，那么 ZXSEC US 设备中的 BFD 设置将宣布路由器不在工作状态并根据情况改变路由。BFD 将仍然保持试图连接到路由器并重新建立连接。

一旦连接恢复后，路由将被重新设置。

配置 BFD

BFD 是针对使用 BGP 或 OSPF 路由协议的网络，这样便排除了小型网络。您可以设置在 ZXSEC US 设备中启动 BFD，并设置关闭一个或两个接口的 BFD 设置。

亦或者，您可以明确在每个邻居路由器或接口中启动 BFD。配置 BFD 的方法，您可以根据网络的配置而选择。

超时时段设置非常重要，且不同的网络与不同型号的 ZXSEC US 设备设置不同。高端 ZXSEC US 设备在流量不超载的情况下反应速度比较快。网络范围的情况也会制约反应的速度，相对小型网络，大型网络的数据包要经过更多的中继。这两个因素（CPU 容量语网络穿越时间）将影响超时时间段的设置，超时设置较短的话，BFD 将不能连接到网络设置，但是 BFD 仍将保持试图连接状态。这种状态便造成不必要的网络流量，且将网络设置置于没有监控的状态下。如果如上所述的情况，您可以试着设置较宽松的超时设置，BFD 便可以有更多的时间检测网络中的设备。

配置 BFD

以 BDF 在 ZXSEC US 设备中使用默认的值启动为例。这就是说，一旦建立了连接，ZXSEC US 设备在 150 毫秒（50x3）内没有得到 BFD 路由器的回应，便宣布路由器不工作以及重新路由流量。BDF 流量发出的端口处于安全考虑将被检测。

config system settings set

bfd enable

set bfd-desired-min-tx 50 set

bfd-required-min-rx 50 set

bfd-detect-mult 3

set bfd-dont-enforce-src-port disable end



注意：

最小接收间隔(bfd-reguired-min-rx)与检测增强(bdf-detect-mult)结合可以判断 ZXSEC US 设备在宣布邻居路由器不工作之前等待回应的时间段设置。正确的设置值根据网络的范围与 ZXSEC US 设备 CPU 运行的速度不同而不同。这里举例的设置值可能不符合您配置网络的情况。

配置端口关闭 BDF

以上的举例是配置在 ZXSEC US 设备中启动 BFD。如果有一个接口不与任何启动了 BDF 的路由器连接，您可以关闭接口的 BFD 设置减少网络流量。例如，使用 CLI 关闭内部接口的 BDF 设置。关闭的方法如果启动或设置 ZXSEC US 设备的默认设置（全局）一样。

config system interface edit

internal

set bfd disable

end

在 BGP 中配置 BFD

在 BGP 网络中配置 BFD 很直观，启动 BFD 设置。BGP 中，您对运行 BGP 协议的每个邻居启动 BFD。这样便允许建立两条通信连接。

在 OSPF 中配置 BFD

在 OSPF 网络中配置 BFD 如同在 ZXSEC US 设备中启动 BFD，您可以通过全局设置启动以及在接口的级别启动。

第12章 路由监控

12.1 概述

描述

本章就如何截取路由监控表的内容进行描述。该列表是用于显示 ZXSEC US 设备中路由表条目的。

内容

12.2 显示路由信息

默认情况下，所有的路由都将在路由监控表中显示。默认的静态路由定义为 0.0.0.0/0，该路由与目标地址为任意的设置的数据包相匹配。

进入路由>监控，显示路由表中的全部路由信息。下图所示是具有接口名为“port1”“port4”与“lan”设置的 ZXSEC US 设备所显示的路由监控列表。您所管理的 ZXSEC US 设备的接口名称设置可能不同。

路由监控表

类型：所有　网络地址：　网关：　启用过滤器

1 / 1

类型	子类型	网络地址	路径长度	路径成本	网关	接口	持续时间 (d h:m:s)
静态		0.0.0.0/0	10	0	10.16.13.3	port2	
直连		10.16.13.0/24	0	0	0.0.0.0	port2	

图12.2-1　路由监控列表

参数名称	参数说明
类型	点击设置在路由列表中搜索以下的路由类型。 ● 设置为“全部”将显示路由表中所记录的路由信息。 ● 设置为“连接”将显示与 ZXSEC US 设备接口之间发生通信的全部路由。 ● 设置为“静态”将显示全部手动添加在路由表中的静态路由。 ● 设置为“RIP”将显示通过 RIP 设置获得的全部路由。 ● 设置为“OSPF”将显示通过 OSPF 设置获得的全部路由。

参数名称	参数说明
	● 设置为“BGP”将显示通过 BGP 设置获得的全部路由。 ● 设置为“HA”则显示 HA 群集设置下主设备与从属设备同步的 RIP，OSPF 以及 BGP 路由。HA 路由信息保存在从属设备中；该路由信息只有从配置在虚拟群集中作为从属虚拟域中查看有关HA路由同步的信息，参见 ZXSEC US 设备 HA 属性用户使用手册。
网络地址	输入搜索路由表的网络 IP 地址与掩码（例如 172.16.14.0/24）并显示与指定网络相匹配的路由。
网关	输入搜索路由表的网络 IP 地址与掩码（例如 172.16.12.1/32）并显示与指定网关相匹配的路由。
启用过滤器	按照指定的搜索规则在路由表中搜索条目并显示匹配的路由。
类型	路由类型。（静态、连接、RIP、OSPF 或 BGP）
子类型	OSPF 中应用的子类型路由。 ● 子类型为空表示该路由是区域内路由。目的地是与 ZXSEC US 设备连接的区域内部。 ● 子类型显示为“OSPF inter area”表示目的地在 OSPF 自主域内，但是 ZXSEC US 设备不与该区域连接。 ● 子类型显示为“External 1”表示目的地在 OSPF 自主域之外。重新分配路由的量度是外部量度与 OSPF 量度相加的和。 ● 子类型显示为“External 2”表示目的地在 OSPF 自主域之外。重新分配路由的量度等于外部量度，用一个 OSPF 量度表示。 ● 子类型显示为“OSPF NSSA 1”与显示为“External 1”表示的含义一样，只是路由是通过 NSSA 区域被接收的。 ● 子类型显示为“OSPF NSSA 2”与显示为“External 2”表示的含义一样，只是路由是通过 NSSA 区域被接收的。
网络地址	ZXSEC US 设备可以到达的目标网络的 IP 地址与掩码。
管理距离	路由有关的管理距离。该数值设置为 0 表示到达相同目标地址该路由是最佳的路线。 有关修改分配到静态路由的管理距离，参见“在路由表中添加静态路由”。或参考 ZXSEC US 设备 CLI 使用参考手册中有关动态路由的内容描述。
路径长度	路由度量路由度量是 ZXSEC US 设备动态选择路由并将路由添加在路由表中的根据。 ● 路由跳数是从 RIP 获得的。 ● 路由相对度量是从 OSPF 获得的。 ● 路由度量使用的多出口标识（MED）是从 BGP 获得的。但是，除了 MED 还有其它几项属性决定到一个目标网络的最佳路径。
网关	到达目标网络网关的 IP 地址。
接口	将数据包转发到目的网络网关的接口。
持续时间	通过 RIP，OSPF 或 BGP 获得路由的时间。

12.3 搜索 ZXSEC US 路由表

您可以应用过滤原则搜索路由列表并显示符合规则的路由。例如，您可以指定显示静态路由，连接路由，从 RIP、OSPF 或 BGP 获得的路由，或与您指定的网络或网关发生通信的路由。

如果您通过设置路由类型搜索路由表或进一步根据网络或网关作为约束所查找的路由，您所设定的作为搜索规则的值必须与相同路由表条目中对应的值相匹配，所搜索的条目才能够显示。（您设定的所有搜索参数都应用了“与(AND)”条件，即对列出的搜索参数默认了都要满足的条件）。

例如，如果 ZXSEC US 设备与网络 172.16.14.0/24 连接，您想查看所有与网络 172.16.14.0/24 直接连接的路由您必须在类型列表中选择“连接”并在“网络”字段输入 172.16.14.0/24然后点击“应用过滤”显示满足以上条件的路由列表条目。“类型”字段中包含关键字“连接”的所有条目以及在“网关”字段与设定条件符合的条目都将显示。

搜索 **ZXSEC US** 路由表

1. 进入路由>当前路由>路由监控表。

2. 在“类型”列表中选择所有搜索的路由类型。例如，选择“连接”将显示所有连接的路由，或选择“RIP”显示所有从 RIP 获得的路由。

3. 如果您想显示到具体网络的路由，在“网络”字段输入该网络的 IP 地址与掩码。

4. 如果您想显示到具体网关的路由，在“网关”字段输入该网关的 IP 地址。

5. 点击“应用过滤”。



注意：

所有您设定作为搜索规则的数值必须符合对应相同路由表中的数值以便能够搜索到路由条目。

第13章 防火墙策略

13.1 概述

描述

防火墙策略控制所有通过 ZXSEC US 设备的通信流量。添加防火墙策略控制 ZXSEC US 接口、区域以及 VLAN 子接口之间的连接与流量。

内容

13.2 关于防火墙策略

防火墙策略是 ZXSEC US 设备决定如何处理连接请求的指令。当防火墙收到一个数据包内发出的连接请求时，ZXSEC US 提取这个数据包的源地址、目的地址和服务（端口号）进行分析。

对于通过 ZXSEC US 设备传输数据包，必须在 ZXSEC US 设备上添加一个与该数据包源地址、目的地址和服务相匹配的防火墙策略。该策略指导防火墙如何处理这个数据包。处理方式可以是允许连接、拒绝连接、在连接前要求认证，或将数据包作为 IPSecVPN 包处理。

每条策略可以单独配置在路由连接或者应用网络地址转换（NAT: network address translation）对源地址、目的地址和端口进行转换。您可以添加 IP 池在防火墙转换源地址时使用动态 NAT。使用策略配置通过 ZXSEC US 的端口实现地址转换（PAT:port address translation）。

您可以在策略中设置保护内容表，从而获得对网页、文件传输和垃圾邮件服务的防病毒保护以及 web 过滤和电子邮件过滤服务。详细信息参见"防火墙保护内容列表"。

您也可以对防火墙策略添加日志记录配置 ZXSEC US 设备记录对所有连接使用的策略。

防火墙通过对策略列表的按顺搜索查找匹配策略。您必须将策略列表中的策略按照具体到概括这样的顺序排列。例如，默认的策略一般很概括，因为它与所有的连接都匹配。当您创建新的策略时，您必须将新建的策略放在策略列表中默认的策略之上。也就是说，默认的策略是与所有的连接都适用并匹配的。

策略选项是通过创建或编辑防火墙策略时配置的。根据您所选择的不同的动作，将呈现不同的策略选项。

多播策略

ZXSEC US 设备支持多播策略。您可以使用以下 CLI 命令配置并创建多播策略：

```
config firewall multicast-policy
```

详细信息，参见 ZXSEC US 设备 CLI 使用参考手册。

策略匹配如何生效

当 ZXSEC US 设备的一个接口接收到连接请求时，将先对策略列表进行搜索查找与该连接请求相匹配测策略。ZXSEC US 是根据该连接请求的源与目标地址进行策略选择的。

ZXSEC US 从所选择的策略名单中自上而下按顺序搜索与接收到连接请求所含有的源与目标地址、服务端口以及时间日期相匹配的第一个策略。搜索到的第一项匹配将应用于连接请求。如果没有相匹配的策略，将放弃该连接。一般情况下，防火墙策略是以具体到综合的顺序排列的。

综合性策略是指可以从多重的源与目标地址或从一个地址范围接收连接的策略。综合性策略也能够从多个服务端口接受连接或具有这样的排程即策略能够与一个很宽泛的时间日期相匹配。如果您想在策略列表中添加除综合性策略以外的策略，这些策略必须添加位于综合性策略之上。

例如这样的综合性策略，即允许您内部网络所有的用户访问互联网中的全部服务。如果您想设置屏蔽到互联网中到 FTP 服务器的访问，您应该在综合性策略之上添加拒绝 FTP 连接的策略。该策略将屏蔽 FTP 连接，对其他服务的访问并不与该 FTP 策略相匹配但是与综合性策略匹配。因此，除了屏蔽了 FTP 连接，防火墙配置仍然从内部网络接受对互联网其他服务的访问。

有关策略匹配的内容还需要作以下说明：需要验证的策略必须添加到策略列表中不需要验证的策略之前；否则，不需要验证的策略将首先被选中。

IPSec VPN 隧道模式策略必须添加在策略列表位于接受或拒绝策略之前。

SSL VPN 策略必须添加在策略列表中位于接受或拒绝策略之前。

13.3 查看防火墙策略列表

如果 ZXSEC US 设备中启动了虚拟域，您可以为每个虚拟域分别配置防火墙策略。从主菜单中点击每个虚拟域可以访问配置的策略。您可以在策略列表中添加、编辑、排序以及启动或断开每项防火墙策略。

进入防火墙>策略项下，可以查看防火墙策略列表。

策略

新建 [列设置]

状态	序号	源地址	目的地址	时间表	服务	保护内容表	动作
loop1 -> port2 (1)							
port1 -> port2 (1)							
port2 -> port1 (2)							
port2 -> port2 (1)							

图13.3-1 策略列表举例

策略列表中显示以下信息。请注意一些栏目默认的情况下是不启动的。使用栏目设置添加货删除列表栏。

策略列表中包括以下图标，以及各图标的功能：

参数名称	参数说明
新建	点击新建添加防火墙策略。参见“添加防火墙策略”。
栏目设置	点击用户定制列表。您可以设定显示栏目以及栏目显示顺序。默认的情况下，不显示状态、源接口、目的接口、VPN 通道、验证、注释、标签、计数、日志、索引号。
过滤 ID	策略标示符。策略根据添加到策略中的顺序编号。
源地址	应用该策略的源地址或地址组。参见“防火墙地址”。地址信息也可以从策略列表中编辑。点击地址可以打开地址编辑对话框。
目的地址	应用该策略的目标地址或地址组。参见“防火墙地址”。地址信息也可以从策略列表中编辑。点击地址可以打开地址编辑对话框。
时间表	激活策略的时间。参见“防火墙时间表”。
服务	策略应用的服务。参见“防火墙服务”。
动作	策略与连接请求相匹配后作出的动作。
状态	启动或中止策略启动该策略表示防火墙将应用该策略与向内的连接进行匹配。
源接口	源接口
目的接口	目的接口
VPN 通道	VPN 策略应用的 VPN 通道。
验证	策略使用的用户验证方法。
注释	创建或编辑策略时可以输入注释信息。
标签	防火墙保护内容名称。

参数名称	参数说明
日志	功能框呈绿色显示表示已对策略启动日志记录呈灰色显示表示没有启动日志记录。
计数	ZXSEC US 设备对通过的数据包以及应用的防火墙策略的数据包字节进行计数。例如，5/50B 表示共通过 5 个数据包，其中 50 字节应用了防火墙策略。
删除图标	点击从列表中删除策略。
编辑图标	点击编辑防火墙策略。
插入策略	点击将新添加的防火墙策略插入到某项策略之前。
移动图标	点击在列表中移动策略项。

添加防火墙策略

使用以下步骤在防火墙列表中添加策略。

1. 进入防火墙>策略。

2. 点击“新建”。您也可以在策略列表中选择要插入策略的位置，并在该位置之前的一个策略项中点击插入策略图标便可以将想要添加策略插入到选定的位置了。

3. 选择源与目的接口。

4. 选择源与目的地址。

5. 配置策略。有关配置策略的详细信息，参见“配置防火墙策略”。

6. 点击 OK 确认。

7. 对新添加的策略进行排序，发挥其功能。

在策略列表中更改策略项的顺序

您可以在策略项中移动一个策略项的位置，可以改变策略匹配的顺序。当对一个接口定义了不止一项策略时，位于策略列表中位次较高的策略将首先进行匹配。

防火墙加密策略的顺序是这些策略能够生效的重要保证。防火墙加密策略是优先于常规策略进行匹配的。

在策略列表中更改策略的顺序并不能更改策略的 ID。

1. 进入防火墙>策略。

2. 移动的策略项，并点击该项中的“移至”图标。

3. 选择策略项所要移动到的位置。

4. 点击 OK 确认。

13.4 配置防火墙策略

使用防火墙策略可以定义一项防火墙策略是如何被选择应用于通信会话的，以及定义 ZXSEC US 设备如何处理通信会话中的数据包。

访问防火墙>策略，添加或编辑防火墙策略。

您可以添加 ACCEPT（接受）策略，接受通信会话。您也可以将 accept 策略应用于 ZXSEC US 设备其他的功能模块例如对策略所接受的通信会话所实行的病毒扫描以及验证功能。如果源或目标地址是 IPSec 虚拟接口，accept 策略能够允许接口通过 IPSecVPN 流量。详细信息，参见 IPSec 接口模式"VPN IPSec 概述"。

您也可以添加 DENY（拒绝）策略，屏蔽某种通信会话类型。您可以添加 IPSec 加密策略启动 IPSec 隧道模式允许通过 VPN 流量，以及 SSL VPN 加密策略允许通过 SSL VPN 流量。防火墙加密策略可以决定在 IPSec 或 SSL VPN 会话过程中哪种类型的 IP 流量可以被允许通过。如果防火墙加密策略允许该 IP 流量通过，那么在任何时间 ZXSEC US 设备接口接受到指定类型的 IP 数据包到达本地私有网络的时候，通道将自动发起通过该类型的流量。详细信息，参见"IPSec 防火墙策略选项"以及"SSL-VPN 防火墙策略选项"。

编辑输出策略

源接口/区 loop1
源地址 all 多个
目的接口/区 port2
目的地址 all 多个
时间表 always
服务 ANY 多个
模式 ACCEPT

NAT 动态IP地址池
保持端口号

保护内容表 unfiltered
记录允许流量
授权认证
检测US Desktop是否安装和运行
限制访问：
US Desktop没有安装
US Desktop没有获得授权
受限的用户重定向到ZXSEC US下载页面
流量控制
认证用户的免责声明
重定向网页
注释（最大63个字符）
AV/IPS库已经过期
取消防病毒
取消防火墙
取消Web过滤
受限的用户重定向到ZXSEC US下载页面

图13.4-1 策略选项- NAT/路由模式 ACCEPT 策略

源与目标接口/区域与源与目标地址的通信会话的防火墙策略相匹配。“地址名称”字段与通信会话的源与目标地址相匹配。

通过时间表可以定义防火墙策略启动的时间。服务是将通信会话使用的服务与防火墙策略相匹配。

动作是定义 ZXSEC US 设备如何处理流量的。对流量可以设置为“接受”或“拒绝”的动作或配置防火墙加密策略。

您可以设置剩余的防火墙策略选项（NAT，保护内容列表，流量日志记录，记录非法日志流量，验证与流量控制）设置其它功能选项。可以应用在拒绝流量的防火墙策略。差分服务可以通过 CLI 命令配置。参见 ZXSEC US 设备 CLI 使用参考手册中“防火墙”章节。

防火墙策略选项

访问防火墙>策略并点击“新建”添加防火墙策略。您可以配置以下策略选项。

参数名称	参数说明
VLAN 间的策略	（只适用于 ZXSEC US350A 设备）该功能只应用于交换模式。启动后，可以创建防火墙策略控制交换 VLAN 中交换端口之间的流量。必须保持至少一个安全端口可用。详细信息，参见“配置 VLAN 间的防火墙策略”。
源地址	设定与 IP 数据包的发送的源地址进行地址匹配的策略。 接口/区域 设置接收 IP 数据包的接口与区域。进入系统管理>网络，列出了接口与区域的列表，可以对区域或接口进行配置。如果动作设置为 IPSEC，接口将与本地私有网络通信。如果动作设置为 SSL-VPN，接口接收远程 SSLVPN 用户的连接。 地址名称 点击之前定义的与源接口或区域发送通信的地址名称。或点击“新建”定义新的 IP 地址。一个数据包的包头必须具有将与策略进行匹配的通信 IP 地址。如果动作设置为 IPSEC，该地址是主机的私有 IP 地址。如果动作设置为 SSL-VPN，该策略只应用于 web 模式的用户，并将地址名称设置为“全部”。如果动作设置为 SSL-VPN，并且策略是针对隧道模式用户设置的，那么选择的地址名称应该是为隧道模式用户保留的地址。
目标地址	设定与 IP 数据包的发送的目标地址进行地址匹配的策略。 接口/区域　　设置转发数据包设备接口与区域的名称通过系统网络页面可以配置接口与区域的设置。 动作设置为 IPSEC，该接口是 VPN 隧道入口。 动作设置为 SSL-VPN，该接口与本地私网连接。 地址名称　　点击之前定义的与目标接口或区域发送通信的地址名称。或点击“新建”定义新的 IP 地址。一个数据包的包头必须具有将与策略进行匹配的通信 IP 地址。 如果动作设置为 IPSEC地址是数据包被发送到 VPN 隧道终端的私有 IP 地址。 如果动作设置为 SSL-VPN，选择位于 ZXSEC US 设备之后的主机，服务器或网络的 IP 地址名称。

时间表	设置固定的时间表或循环的时间表以控制与通信会话匹配的策略生效的时间。访问防火墙>时间表可以预先设置时间表。参见"防火墙时间表"。 您也可以点击新建在策略配置时创建新的固定或循环时间表。设置完成后点击 OK，新的时间设置将被添加在时间列表中。
服务	设置与数据包传输使用的服务与协议相匹配的服务与服务组的名称您可以从预先定义的服务中选择或添加用户服务或服务组。进入防火墙>服务>用户定制服务，可以预先创建用户定制的服务。或在防火墙服务同一菜单下，进入服务组也可以预先配置服务组设置。详细信息，参见"配置用户定制服务"以及"配置服务组"。 您也可以点击新建在策略配置时创建新的用户定制服务或服务组。设置完成后点击 OK，新服务将被添加在服务列表中。 点击"多选"，可以选择多个服务或服务组。
动作	设置当数据包与策略匹配时，防火墙采取的动作。 接 受　接受与该策略相匹配的连接。您也可以配置 NAT、内容保护表、流量日志、流量控制、授权认证以及差分服务。您也可以在策略中添加注释。 拒绝**(DENY)** 设置为拒绝便丢弃了与策略相匹配的连接。您可以配置的唯一的其它策略选项是流量日志（记录被该策略拒绝的连接）与差分服务。您也可以在策略中添加注释。 IPSEC 配置 IPSec 防火墙加密策略，使 ZXSEC US 设备能够处理 IPSec VPN 数据包。参见"IPSec 防火墙策略选项"。 SSL-VPN 配置 SSL-VPN 防火墙加密策略，使 ZXSEC US 设备能够处理 SSL VPN 流量。该设置选项只有在您添加了 SSL-VPN 用户组后才需要配置的。参见"SSL-VPN 防火墙策略选项"。

NAT	对防火墙策略启动网络地址转换NAT 设置将策略接受的源地址与数据包的端口进行转换。启动 NAT 设置后，可以配置动态 IP 池与保持端口号。透明模式下，NAT 设置不可用。 动态 **IP** 地址池 设置为动态 IP 池将源地址转换成为从 IP 池中选择的任意一个地址。IP 池可以是单个的 IP 地址或一个 IP 地址的范围。目标接口或区域中添加了 IP 池后向显示一个 IP 池列表。 点击 ANY IP 池，ZXSEC US 从添加到目标接口或区域中 IP 池中选择任意的 IP 地址。 点击添加到目标接口或区域的 IP 池名称，ZXSEC US 设备将源地址转换为该 IP 池定义的任何一个地址。 如果目的接口，VLAN 子接口或目标区域中的接口或 VLAN 子接口配置使用了 DHCP 或 PPPoE 则不能选择动态 IP 地址池。 使用区域时不能配置使用 IP 池。 有关添加 IP 地址池的详细信息，参见"IP 地址池"。 保持端口号 点击"保持端口号"，防止 NAT 转换源端口。如果源端口被更改，一些应用将不能正常工作。多数情况下，如果您选择了"保持端口号"，需要同时设置为动态 IP 池。如果不设置为动态 IP 地址池，设置了固定端口的策略一次只允许一个连接通过。
保护内容表	选择保护设置配置并在防火墙策略中应用反病毒，web 过滤，网页类型过滤，反垃圾邮件，IPS，内容存档以及日志服务。有关添加与配置内容表的详细信息，参见"内容保护表"。 如果在高级设置中配置用户认证因为从验证中选择的用户组已经与内容保护表绑定，所以不需要设置内容保护表。详细信息，参见"对防火墙策略设置验证"。
日志记录允许通过的流量	对动作设置为"ACCEPT，IPSEC 或 SSL-VPN"允许通过的流量进行日志记录。您也可以设置流量日志存储的位置 （syslog,Web Trends,可用的本地硬盘，内存或 USLA 设备）并将日志的威胁级别设置为"告知"或"较低"。有关日志的详细信息，参见"日志与报告"。
日志记录非法流量	对动作设置为"DENY"拒绝通过的流量进行日志记录。您也可以设置流量日志存储的位置（syslog,Web Trends,可用的本地硬盘，内存或 USLA 设备）并将日志的威胁级别设置为"告知"或"较低"。有关日志的详细信息，参见"日志与报告"。
验证	显示验证页面。用户必须接受显示的验证页面。您可以使用验证页面查看验证内容与保护内容表该选项只有在一些型号的设备中可用。
检测是否安装并运行 **US Desktop**	ZXSEC US6010A 与 ZXSEC US5005A 设备中,防火墙可以设置拒绝没有安全并运行 US Desktop 主机安全软件的主机访问功能。

流量控制	流量控制设置宽度的使用，以及优先处理的流量。 在防火墙策略中启动流量控制。如果对策略不应用任何流量控制规则，默认情况下该策略具有最高的优先级。 将防火墙策略设置为三个优先级别。（低、中、高） 查看为策略所设置的宽度流量低于接口的最大带宽容量。
用户验证免责声明	显示验证免责声明页面（替换信息）。用户必须点击"接收"声 明信息从而连接到目标地址您可以使用免责声明与验证或内容保护列表结合。该选择在一些 ZXSEC US 设备型号中可用。 对于 SSL-VPN 策略不可用。
URL 重新定向	在您接受验证和/或接受用户验证信息内容后，用户将被重新定向到一个 URL。该选项只有在一些型号的设备中可用。
注释	您可以对策略添加描述性或其它的信息。描述信息描述包括空格可以为 63 个字符的长度。

配置 VLAN 间的防火墙策略（只适用于 ZXSEC US350A）

交换模式下，可以创建防火墙策略控制交换 VLAN 中交换端口之间的流量。这些策略称为交换 VLAN-安全策略。在 VLAN 间创建策略的详细信息，参见"防火墙策略选项"。

VLAN 间的策略必须保留至少一个安全端口作为源或目标端口。在两个不安全的端口之间不可能创建防火墙策略。有关创建安全交换端口的详细信息，参见"配 置交换-VLAN 接口"。

进入"防火墙>策略"并点击"新建"配置新的防火墙策略。

图13.4-2 创建 VLAN 间的防火墙策略

参数名称	参数说明
VLAN 间的策略	启动该设置创建交换端口之间策略启动该设置后显示以下的字段。
源/目标接口/区域	点击设置本地或交换 VLAN。创建交换 VLAN 的详细信息，参见“配置交换 VLAN”。
源与目标端口	端口　点击设置为“任何”或具体一个交换端口。如果您设置一个非安全端口作为源端口您必须设置一个安全端口作为目标端口。 地址　点击设置为“全部”或设置一个 IP 地址范围。根据需要设置其它防火墙选项。参见“防火墙策略选项”。

配置防火墙策略的验证设置

设置验证之前，您必须在用户组添加用户与防火墙保护内容设置。有关添加与配置用户组的详细信息，参见“用户组”。只有将动作设置为“接受（Accept）”或 SSL VPN 后，才需要配置验证选项。

当您在防火墙策略中启动用户验证时，使用防火墙策略的终端用户在使用策略之前将被要求接受验证。

选中验证功能框并选择一个或多个用户组，防火墙接受连接之前，用户需要输入用户名与密码。

如果使用证书验证（只适用于 HTTP 或 HTTP 重新定向到 HTTPS），您可以在 ZXSEC US 设备中安全定制的证书并且终端用户也可以在浏览器中安装定制的证书。否则，终端用户将看到警告信息并不得不接受用户使用的浏览器可能认为是非法的默认的 ZXSEC US 设备的证书有关如何使用用户证书的信息，参见“VPN 证书”。



注意：

在您使用证书验证时，创建策略时不指定任何证书，那么将使用全局设置。如果您指定了证书，基于每项策略设置将覆盖全局设置。有关用户验证全局设置的详细信息，参见“验证设置”。

用户验证支持以下协议：

HTTP

HTTPS

Telnet

FTP

配置验证协议与其它验证设置的信息，参见“验证设置”。

您可以选择对任何服务的认证用户可以在防火墙上使用 HTTP、Telnet 或者 FTP 认证。为了让用户通过认证，必须为认证配置添加 HTTP、Telnet 或者 FTP 策略。当用户试图通过防火墙使用这个策略连接时，将会被提示输入防火墙用户的用户名和密码。

防火墙验证方式包括在本地定义用户组以及 LDAP 与 Radius 用户进入用户>用户组，点击活动目录从下拉的菜单中选择目录。设置有活动目录组与其他用户组的验证不能够在同一个策略中结合。

您可以指定哪种协议用于发布验证请求。防火墙策略必须包括终端用户能够被验证的验证协议。例如，如果您创建 POP3 策略且您指定使用 HTTP 协议进行验证，防火墙策略服务必须包括至少 HTTP 与 POP3。

编辑用户组

名称 test1

类别 防火墙

保护内容表 scan

可用的成员

- 本地用户 -
- RADIUS/LDAP/TACACS+ 服务器用户 -
- PKI用户 -

組员

- 本地用户 -
test
- RADIUS/LDAP/TACACS+ 服务器用户 -
- PKI用户 -

跳过US Service Web过滤

返回

图13.4-3　选择验证的用户组

设置验证或设置一个或多个用户组要求用户输入用户名与密码，或在防火墙接受连接之前使用证书进行验证。

防火墙验证方式包括本地定义的用户组以及 LDAP 与 RADIUS 用户。从下拉菜单中点击活动目录，选择“用户>用户组”中定义的活动目录组。使用活动目录组进行的验证不能与其他组结合在相同的策略中。

使用 NTLM 验证，从下拉菜单中点击 NTLM，选择“用户>用户组”中定义的活动目录组。您使用 AD 组作为 NTLM 验证组的成员。



注意：

配置允许 ZXSEC US 设备使用活动的目录服务器验证，中兴通讯服务器验证扩展（FSAE）必须安装在活动目录域名控制器上。从中兴通讯技术支持可以获得 FSAE。

多数情况下，您必须确定用户无须认证就可以通过防火墙使用 DNS。如果 DNS 不可用，用户将无法使用域名访问网页服务、FTP 或者 Telnet。



注意：

需要认证的策略必须添加在策略列表中不需要验证的策略之上；否则不需要验证的策略将先被选择。

配置策略的流量控制

流量控制配置可以控制可用的宽带流量以及设置防火墙策略处理流量的优先级别。在大量的数据通过 ZXSEC US 时，流量控制可以设置哪个策略具有更高的处理优先权。例如，为公司的 web 服务器设定的策略可能分配比大多数为雇员电脑设定的策略具有更高的优先级。当一个雇员需要使用比平常更快的互联网访问速度时，可以为他设置一个具有较高带宽的特定的向外连接策略。

流量控制设置只有对设置动作为 Accept，IPSEC 以及 SSL-VPN 的策略可用。在一些所支持的服务如 H.323，TCP，UDP，ICMP 以及 ESP 中也可以配置流量控制。在未来发行的版本中，对于 SIP 也可以设置流量控制。

基本保证与最大宽度设置相结合的队列可以保证流量的最小与最大带宽的使用。流量控制并不能够增加总的带宽的可用量，但是该设置能够密集型带宽以及敏感性流量使用质量。



注意：

有关流量控制的详细信息，参见“ZXSEC US 设备流量控制参考”。

基本带宽保证与最大带宽的使用

使用流量限制可以确保一项策略允许通过防火墙的流量具有一定的可用宽带。基本宽带（以 kbps 为单位）确保对优先级高的服务有足够的带宽可用。例如，您可以对电子商务流量设置较高基本带宽使用量。

防火墙策略所控制的流量可用的带宽可以同样用于控制双向的流量。举例说明，如果对从内部到外部网络的 FTP 策略的基本带宽使用值，并且内部网络的用户同时使用 FTP 放取文件，那么放取文件的通信会话将共享防火墙策略中所设置的流量限制设置。

为一项策略设置的基本带宽与最大带宽也就是该策略控制的通过的流量能够使用的全部可用带宽。如果多个用户使用相同的策略发起多个通信会话，所有这些通信会话将共享该策略所控制的带宽使用。

但是，如果不同策略控制下的多个用户使用相同的服务，那么他们之间不需要共享带宽。举例说明，您可以创建一项 FTP 策略对一个网络地址限制 FTP 可用的带宽同时创建另一项 FTP 策略对于另一个网络地址设置不同的可用带宽。

流量优先级设置

设置流量的优先级，以管理不同类型的流量。对于重要以及潜在敏感的流量应该设置较高的优先级。对于不是很重要以及敏感度不高的流量分配较低的优先级。

ZXSEC US 设备中反病毒功能模块中的带宽设置只有当优先级高的连接不需要时才对优先级较低的连接可用。

例如，连接到一个安全的 web 服务器的策略用于语音传输以及电子商务通讯的流量应该设置为基本带宽。您可以对控制语音流量的策略设置较高的优先级，将控制电子商务的的策略设置为中等优先级。网络通信繁忙时，如果语音流量与电子商务流量同时占用带宽时，优先级设置较高的语音流量将先于电子商务流量被传输。

流量控制配置注意事项

流量控制配置意在流量高峰时均衡流量并配置某些类型的流量优先于其他流量使用带宽。但是，对于一些存储在缓存中数据类型以及能够在缓存中存储的时间限制。一旦超出了这些限制，数据包就被丢弃，通信会话将受影响。流量控制配置不当将可能降低某些网络流，因为大量的数据包被丢弃对上层网络带来额外的开销，这些开销是用来纠正错误的。

流量控制的基本原则是在牺牲一些能够被丢弃的数据包的基础上优先某些数据流量。也就是说，您设置放弃了流量 X 的性能与稳定性，是为了保证流量 Y 的性能与稳定性。

举例说明，如果您对某些数据流设置了带宽限制，必须明白这样的事实，这些会话将被限制流量，而且可能会话质量受到影响。

对防火墙策略应用流量控制，也就是对通过该策略的双向流量设置了带宽使用。例如内部主机发起的到外部主机的会话通过内部到外部网络的防火墙策略，那么从外部网络返回到内部网络的数据流也要应用对通过的防火墙设置的流量控制。例如，使用 FTP 放取文件或 SMTP 服务器与外部主机连接获取电子邮件。

流量控制功能同样作用于正常流速的常规 IP 流量。在流量相当高的情况下，也就是在超出了 ZXSEC US 设备能够处理的情形下，流量控制功能将不再生效。ZXSEC US 设备先要接收数据包流量，然后对流量应用流量控制功能。如果 ZXSEC US

不能够处理接收的全部流量，可能会发生丢弃数据包、延迟处理数据包这样的情况。

为了保证流量控制能够发挥最佳性能，确保接口以太网统计表没有错误、数据包冲撞以及缓存超容这样的事件。如果统计表不是清洁的，ZXSEC US 设备与交换机可能需要调整。

为了流量控制功能更能有效地发挥，需要注意以下几项设置规则：在防火墙启动流量控制设置。如果您不对防火墙策略设置任何的流量控制，那么默认情况下，流量的优先级别设置为高级。将防火墙策略中的流量控制选项设置为三个优先级别（低、中、高）。

确定防火墙策略中所有基本带宽之和需要低于接口多承载的最大容量。在配置防火墙策略的同时可以配置流量控制选项。

配置流量控制设置

进入防火墙>策略。当您创建新的策略或编辑一项策略的同时，设置流量控制选项。配置以下选项：

参数名称	参数说明
基本带宽	使用流量限制可以确保一项策略允许通过防火墙的流量具有一定的可用宽带。保证宽带(以 kbps 为单位)确保对优先级高的服务有足够的带宽可用。
最大带宽	您也可以使用流量限制限制一项策略允许通过防火墙的流量的宽带使用量限制带宽流量保持重要性较高的服务相比重要级别较低的服务拥有良好的宽带使用。
优先级	数据流优先级别设置为三个级别，分别为高、中、低。选择不同的优先级，ZXSEC US 设置可以针对不同的流量类型设置相应的优先级别。例如，连接到一个安全的 web 服务器的策略用于支持电子商务通讯流量，应该设置为较高的优先级别而对于重要程度较低的服务应当标上较低的优先级别防火墙分配宽带的原则是当高优先级的连接不再占用带宽时，防火墙才会将带宽分配给低优先级的连接。



注意：

如果您同时将基本带宽与最大带宽设置为零，那么策略将不允许任何流量通过。

IPSec 防火墙策略选项

当防火墙策略的动作选项设置为 IPSEC 时，需要相应配置以下设置。

参数名称	参数说明
VPN 通道	选择在阶段 1 配置中定义的 VPN 通道名称。所指定的通道将应用该项防火墙加密策略。
允许向内	允许远程私网的拨号用户或计算机发起的通道的连接流量。
允许向外	允许本地私网的计算机发起的通道连接流量。
向内 NAT	点击该选项将向内加密的数据包的源 IP 地址转换成为 ZXSEC US 接口的 IP 地址发送到本地私网。
向外 NAT	点击该选项与 natipCLi 值结合将向外纯文本文件的数据包地址转换成为您指定的 IP 地址。除非您通过 CLI 指定了 natip 值否则不要选择向外 NAT 选项。指定 natip 值时向外 IP 数据包的源地址将被在数据包通过通道发送之前被代替。详细信息，参见 ZXSEC US 设备 CLI 使用参考手册中“防火墙”章节。



注意：

基于路由的 IPSec 通道的配置方式与通道模式的 IPSec 配置方法不同。不同于定义防火墙加密策略允许 VPN 连接与通过通道控制 IP 流量；您可以将基于路由的 VPN 通道与 IPSec 虚拟接口绑定，并在常规防护墙策略中指定 IPSec 虚拟接口作为源与目标接口。

详细信息，参见 ZXSEC US 设备 IPSec VPN 用户使用手册中“定义防火墙加密策略”章节。

SSL-VPN 防火墙策略选项

当防火墙策略的动作选项设置为 SSL-VPN 时，需要相应配置以下设置。



注意：

创建一个或多个 SSL VPN 用户组以后，可以从动作列表中设置 SSL-VPN 选项参见页“配置 SSL-VPN 用户组选项”有关创建用户帐户与 SSL VPN 用户组。

SSL客户端认证限制
加密强度 Any
User授权方法 Any
可用组: 允许的:
testvpn

图13.4-4 SSL-VPN 加密策略

参数名称	参数说明
SSL 用户证书限制	允许持有用户证书产生的流量通过。持有组证书的用户必须是 SSL VPN 用户组的成员，并且用户组的名称必须在“允许”字段显示。
密钥长度	设置以下的 SSL 加密使用的选项。远程用户的 web 浏览器必须能与您设置的密钥相匹配。 ● 使用任何密钥对，设置为“任何”。 ● 使用 164 位或更高的密钥对，设置为“大于等于 164”。 ● 使用 128 位或更高的密钥对，设置为“大于等于 128”。
用户验证方式	设置为以下任何一种选项： ● 如果用户组与该防火墙策略绑定的是本地用户组，设置为“本地”。 ● 如果远程用户通过外部 RADIUS 服务器认证，设置为“Radius”。 ● 如果远程用户被外部 LDAP 服务器验证，设置为 LDAP。 ● 设置为“任何”将启动以上所有的认证方式。使用“本地，Radius 以及 LDAP”顺次逐个验证。
可用组选项	使用向右箭头选择需要 SSL VPN 访问的用户组名称。除非用户组具有相同的访问需求，否则不要选择多余一个的用户组。

有关对 SSL VPN 用户创建防火墙加密策略的详细信息，参见 US SSL VPN 用户使用手册中有关“SSL VPN 管理员任务”章节。

查看主机中安装 US Desktop 的选项

US6010A，5005A 这些设备中，防火墙策略可以拒绝没有安装与运行 US Desktop 主机安全软件的主机访问。该功能可以检测 US Desktop 软件版本 3.0MR2 或之后的版本。

参数名称	参数说明
检测是否安装并运行 US Desktop	检测源主机是否安装并运行了 US Desktop 主机安全软件。由于以下原因可以拒绝主机的访问： ● 没有安全 US Desktop ● US Desktop 没有许可证 ● AV/IPS 数据库过期 ● AV 功能没有启动 ● 防火墙功能没有启动 ● Web 过滤功能没有启动
将受限的用户重新定向到 **US** 下载入口	设置将被拒绝的用户重新定向到内部 web 入口，且提供被拒原因。对于支持该功能的设备，用户可以下载 US Desktop 主机安全软件。

13.5 防火墙策略设置举例

ZXSEC US 设备可以完全满足各种网络的要求，不管是 soho 还是大型企业与 ISP 的需求。以下两个举例分别应用在 soho 与大型企业办公环境中，充分体现 ZXSEC US 设备防火墙策略的功能实现。

在 USOS v3.0 MR2 的操作说明中，参见图书馆网络、SOHO 与 SMB 网络防护部署举例。

- 场景一：SOHO 级别部署
- 场景二：企业级别部署

场景一：SOHO 级别部署

公司 A 是小型的软件公司，开发程序并提供用户支持的业务。另外，公司的内部网络包括 15 部计算机，几个员工全部或部分时间是 soho 的状态。

从公司 A 当前的网络拓扑结构来看，全部的 15 台计算机设备是部署在路由器之后的且必须进入内部源地址访问 IPS Mail 或 web 服务器。所有进行 soho 的员工通过开放/非开放的安全的连接访问路由器。

公司 A 需要进行 soho 的员工能够保证安全的连接。如果许多公司一样，依赖电子邮件的往来与互联网的沟通来传递信息进行业务交流。公司 A 需要配置全方位安全的解决方案，以检测并防止网络攻击、屏蔽病毒与减少垃圾邮件的产生。公司 A 希望对不同的部门应用不同的保护设置。同时要求将 web 与邮件服务器整合到安全解决方案中。

公司 A 对基于 soho 工作的员工配置了具体的策略，以保证基于 soho 之间的员工连接以及内部网的联接是安全的。

1. 进入"防火墙>策略"。

2. 点击"新建"并输入或对 Home_User_1 配置以下的设置：

接口/区域	源接口：internal	目标接口：wan1
地址	源：CompanyA_Network	目标：Home_User_1
时间表	总是（Always）	
服务	任何（ANY）	
动作	IPSEC	
VPN 通道	Home1	
允许进入	是	
允许流出	是	
流入 **NAT**	是	
流出 **NAT**	否	
内容保护列表	启动并设置为 standard_profile	

3. 点击 OK 确认。

4. 点击"新建"并输入或对 Home_User_2 配置以下的设置：

接口/区域	源接口：internal	目标接口：wan1
地址	源：CompanyA_Network	目标：全部
时间表	总是（Always）	
服务	任何（ANY）	
动作	IPSEC	
VPN 通道	Home2_Tunnle	
允许进入	是	
允许流出	是	
流入 **NAT**	是	
流出 **NAT**	否	
内容保护列表	启动并设置为 standard_profile	

5. 点击 OK 确认。

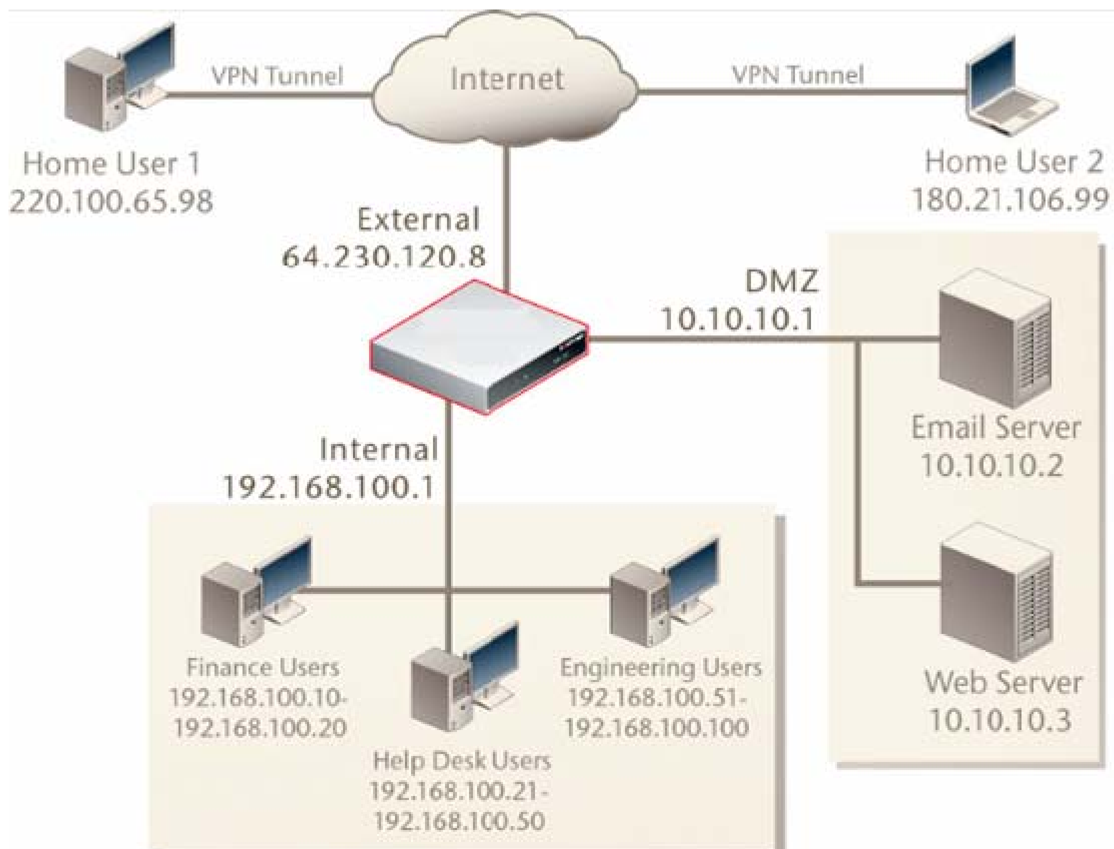


图13.5-1 部署后的 SOHO 网络

部署的网络是根据 ZXSEC US180 来配置的。15 台计算机设备位于 ZXSEC US 设备之后。员工可以在一个 DMZ 中访问邮件与 web 服务器，且 DMZ 位于 ZXSEC US 设备之后。所有 soho 的员工现在通过 ZXSEC US 设备的 VPN 通道访问公司网络。

场景二：企业级别部署

大城市中，数据库系统固定在主城区中，延伸出很多分支，服务于大部分的人。每个分支都连接到互联网，但是分支之间没有任何的设置连接存在。

位于主城区的当前网络拓扑结构由三个用户组组成。主要的分支与公共终端在防火墙之后的 DMZ 内访问服务器。目录直接访问终端，不需要首先通过防火墙再访问目录服务器。

分支结构通过非安全互联网连接访问主干中的服务器。

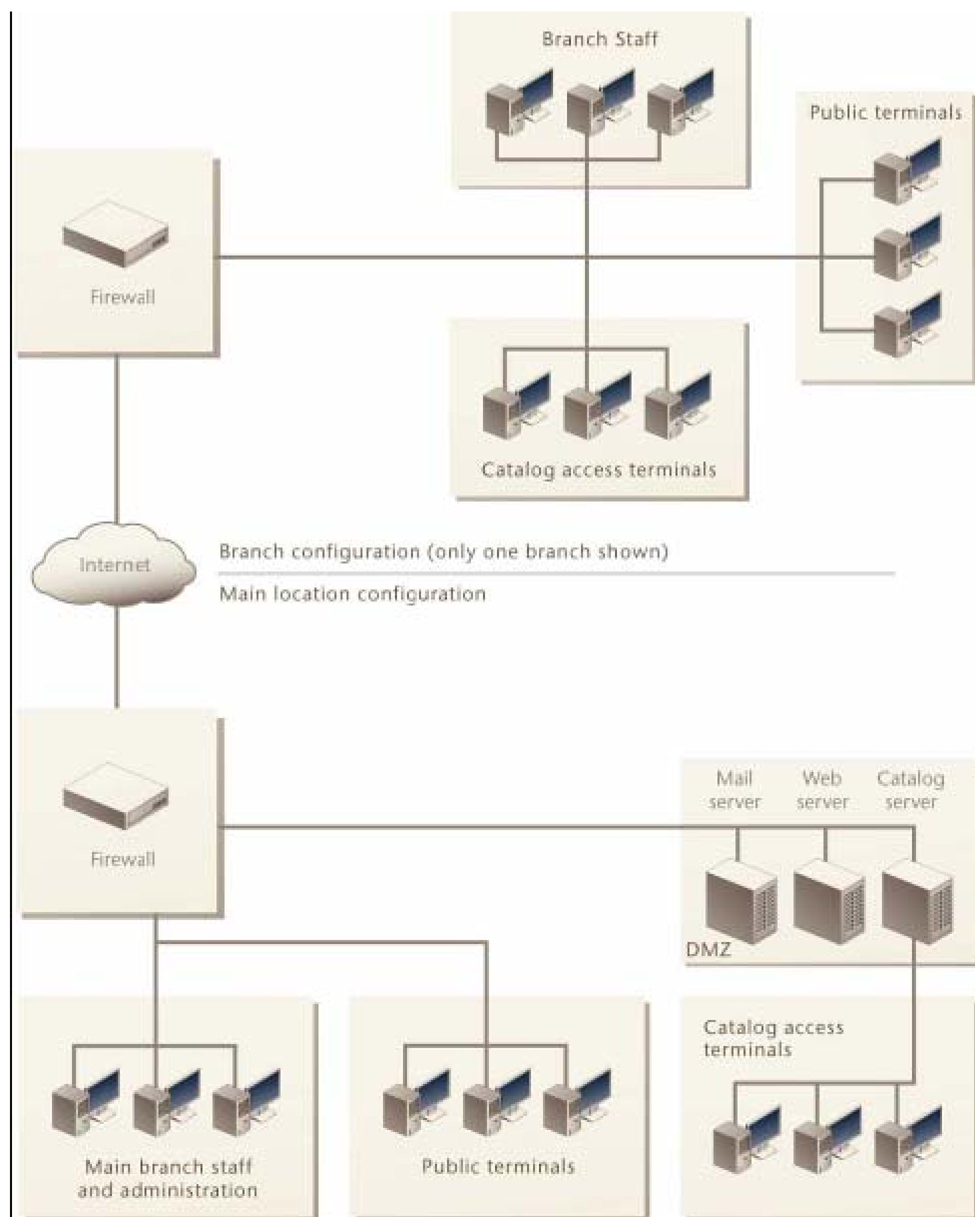


图13.5-2　数据库系统的当前网络拓扑结构

数据库系统必须对用户与访客设置不同的访问安全级别。

第一项对于主办公区人员设置的防火墙策略是允许在任何时间没有限制的访问互联网。第二项策略是允许员工直接访问 DMZ。第二项策略设置允许分支机构的员工具有相同的访问权限。

员工类的防火墙策略将配置使用保护内容列表。保护内容列表中启动的功能包括病毒扫描、IPS 以及屏蔽所有的 P2P 流量。US Service web 过滤功能也用于屏蔽广告、恶意软件以及灰色软件。

很少的用户，根据配置需要，可能会访问特殊的 web 与目录服务器以更新服务器上的信息。特殊的访问可以使用基于 IP 地址或用户进行。

设置的拓扑结构具有主干与目录访问终端,通过一个 US HA 群集访问 DMZ 中的服务器。公共访问终端首先经过一台 USWiFi 设备，USWiFi 设备中可以应用另外的策略，访问 HA 群集最终访问服务器。

分支机构中的所有三部分用户通过一台 USWiFi 路由，经由 VPN 通道访问主干网络。

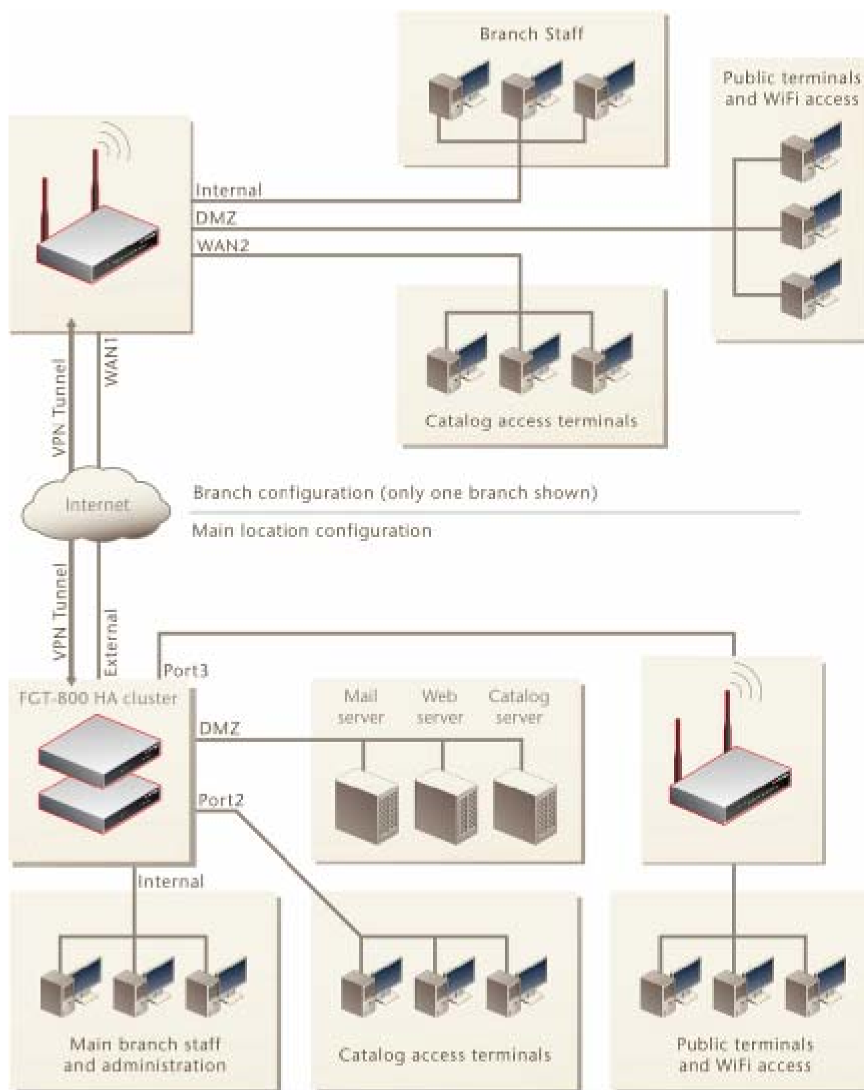


图13.5-3 设计实施的数据库系统网络拓扑结构

进入“防火墙>策略”配置策略。保护内容列表在“防火墙>保护内容列表”中配置。

总公司员工访问互联网的策略设置：

参数名称	参数说明
源接口	Internal（内部）
源地址	全部（All）
目标接口	External（外部）
目标地址	服务器（servers）
时间表	总是（Always）
动作	接受（Accept）

总公司员工访问 DMZ 的策略设置：

参数名称	参数说明
源接口	Internal（内部）
源地址	全部（All）
目标接口	External（外部）
目标地址	全部（All）
时间表	总是（Always）
动作	接受（Accept）

分公司员工访问互联网的策略设置：

参数名称	参数说明
源接口	分支（Branches）
源地址	分支机构员工（Branch staff）
目标接口	External（外部）
目标地址	服务器（servers）
时间表	总是（Always）
动作	接受（Accept）

分公司员工访问 DMZ 的策略设置：

参数名称	参数说明
源接口	分支（Branches）
源地址	分支机构员工（Branch staff）
目标接口	DMZ
目标地址	服务器（servers）
时间表	总是（Always）
动作	接受（Accept）

有关举例的详细信息，参见：

- SOHO 与 SMB 配置举例说明
- ZXSEC US 设备公司配置举例说明

第14章 防火墙地址

14.1 概述

描述

您可以根据需要添加、编辑以及删除防火墙地址。防火墙地址将被添加到防火墙策略的源以及目标地址字段。添加到防火墙策略中的地址是用来与 ZXSEC US 设备接收到数据包的源以及目标地址相匹配的。

内容

14.2 有关防火墙地址

一个防火墙地址可以是：

- 单个计算机的 IP 地址（例如，192.45.46.45）。
- 一个子网的 IP 地址（例如，class C 子网的地址 192.168.1.0）。
- 0.0.0.0.表示所有可能的 IP 地址。

所添加的 IP 地址对应的掩码。例如：

- 单个计算机 IP 地址的掩码应该为 255.255.255.255
- Class A 子网的掩码应该为 255.0.0.0
- Class B 子网的掩码应该为 255.255.0.0
- Class C 子网的掩码应该为 255.255.255.0
- 所有地址的掩码应该为 0.0.0.0 一个 IP 地址范围表示：
- 子网中 IP 地址的范围（如：192.168.20.1 到 192.168.20.10）

注意：IP 地址为 0.0.0.0 与掩码为 255.255.255.255 不是有效的防火墙地址。将地址组织添加到地址组中可以简化策略的创建。可以配置防火墙地址的名称，IP 地址与掩码或一个 IP 地址范围及名称。

一个防火墙地址可以配置为名称、IP 地址与掩码，或名称与 IP 地址范围。同样也可以是完整且合格的域名（FQDN）。

您可以使用如下格式输入 IP 地址与掩码。

- x.x.x.x/x.x.x.x，如 64.198.45.0/255.255.255.0
- x.x.x.x/x，如 64.195.45.0/24

使用以下格式输入 IP 地址范围。

- x.x.x.x-x.x.x.x，如 192.168.110.100－192.168.110.120
- x.x.x.[x-x]，如 192.168.110.[100-120]
- x.x.x.*，如 192.168.110.*代表子网中全部的地址

一个 IP/掩码地址表示为：

- 子网的地址（例如：Class C 子网，IP 地址为：192.168.20.0 以及掩码为

255.255.255.）

- 单个 IP 地址（例如：IP 地址：192.168.20.1 与掩码为 255.255.255.255）
- 所有可能的 IP 地址（用 IP 地址：0.0.0.0.与掩码：0.0.0.0.来表示）

使用以下格式输入 FQDN 地址：

- <主机名称>二级域名<顶级域名>
- <主机名称><顶级域名> 一个

FQDN 可以是：

- www.zte.com.cn
- XXXX.com

14.3 查看防火墙地址列表

如果在 ZXSEC US 设备中启动了虚拟域设置，需要对每个虚拟域配置单独的地址。从主菜单的地址列表中选择虚拟域可以查看每个虚拟域所配置的地址。

将地址添加在地址列表中并编辑已配置的地址。ZXSEC US 设备默认配置的地址“全部”表示网络中任何的 IP 地址。地址列表中是根据类型分类的，IP/掩码，IP 地址范围与 FQDN。

进入防火墙>地址，可以查看地址列表。

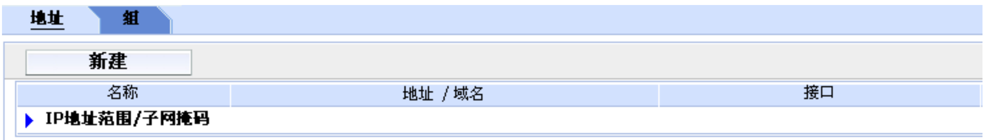


图14.3-1 地址列表示例

参数名称	参数说明
新建	点击新建添加防火墙地址。
名称	防火墙地址的名称。
地址/FQDN	防火墙的 IP 地址与掩码或 IP 地址范围，或有效的域名。
删除图标	选中一项地址，点击删除图标可以将该地址从列表中删除。如果地址应用于防火墙策略则不可以被删除。
编辑图标	点击编辑图标可以编辑地址名称，IP 地址范围或合法域名项目。

14.4 配置地址

通过防火墙策略页面，在配置防火墙策略的同时可以创建或编辑地址。只需要在自动保留一个 FQDN 所含有的全部地址的 ZXSEC US 设备中设置一项 FQDN 策略便可以映射到多台设备用于负载平衡以及 HA。



注意：

在防护墙策略中使用一个完整有效的域名可能带来一些安全威胁。请谨慎使用该策略。

进入防火墙>地址，可以添加 IP 地址、IP 地址范围或 FQDN。

新建地址
地址名称
类型 子网/IP范围
子网/IP范围 0.0.0.0/0.0.0.0
接口 任意
OK 取消

图14.4-1 创建新地址或 **IP** 地址范围的选项

参数名称	参数说明
地址名称	输入防火墙地址的名称。地址，地址组以及虚拟 IP 必须设置唯一性的名称避免与防火墙策略中的地址相混淆。
类型	设置地址的类型为：子网/IP 地址范围或 FQDN。
IP 地址范围**/**掩码	输入防火墙 IP 地址/子网掩码或输入使用分隔符相间的 IP 地址范围。
接口	设置接口与配置的 IP 地址建立对应关系。如果当您在创建策略时将 IP 地址与接口/区域连接时，设置为“任何”。

14.5 查看地址组列表

如果在 ZXSEC US 设备中启动了虚拟域设置，需要对每个虚拟域配置单独的地址组。从主菜单的地址列表中选择虚拟域可以查看每个虚拟域所配置的地址组。

您可以将相关的地址编入地址组中方便配置策略。例如，如果您添加三个地址并在地址组中对地址进行配置，您可以使用这三个地址配置一个策略。

注意：

如果策略组中包含一个地址组，必须先从策略中移除该地址组然后才可以删除。

地址 组
新建
组名 成员

图14.5-1 地址组列表示例

地址组中包含的图标以及地址组的功能：

参数名称	参数说明
新建	点击新建地址组。
组名	地址组的名称。
成员	地址组中的成员。
删除图标	点击从列表中删除地址组。只有在地址组没有用于防火墙策略时才可以被删除。
编辑图标	点击编辑地址组名称以及成员地址项。

14.6 配置地址组

从地址项的下拉列表中点击新建可以创建地址组。

进入“防火墙>地址>组”，可以将地址编入地址组中。

新建地址组
组名
可用地址:
12
all
成员:
OK
取消

图14.6-1　地址组选项

地址组具有以下选项：

参数名称	参数说明
组名称	输入地址组的名称。地址，地址组与虚拟 IP 必须设置唯一的名称避免与防火墙策略中的地址混淆。
可用地址	可配置的列表与默认的防火墙地址。使用上下箭头在两个列表中相互移动地址。

成员	组中的地址列表。使用上下箭头在两个列表之间移动地址。

第15章　防火墙服务

15.1 概述

描述

设置服务识别防火墙接收或拒绝的通信会话类型。您可以在策略中添加任何预先定义的服务。您也可以创建用户服务或在服务组中添加服务。

内容

15.2 查看定制服务列表

如果 ZXSEC US 设备配置启动了虚拟域,预先定义的服务可以在全局配置中进行设置。

在主菜单项下，点击全局配置，进入防火墙>服务，可以查看预先定义的服务列表。

预定义　定制　组

名称	描述
AH	IP/51
ANY	ALL
AOL	TCP/5190-5194
BGP	TCP/179
DCE-RPC	TCP/135 UDP/135
DHCP	UDP/67-68
DNS	TCP/53 UDP/53
ESP	IP/50
FINGER	TCP/79
FTP	TCP/21
FTP_GET	TCP/21
FTP_PUT	TCP/21
GOPHER	TCP/70
GRE	IP/47
H323	TCP/1720,1503 UDP/1719

图15.2-1　定制服务列表

定制服务列表中图标及其功能。

参数名称	参数说明
服务名称	预先定义服务的名称。
详述	每条定制服务的协议。

表 33 列出的是 ZXSEC US 定制的防火墙服务。您可以将这些服务添加到任何策略中。

表 **33**：定制服务列表

服务名称	描述	协议	端口
ANY	与任何端口的连接匹配。使用任何定制服务的连接都允许通过防火墙。	全部	全部
GRE	通用路由封装。一个协议通过封装 GRE 数据包内的数据包协议允许任意的网络协议基于任何其它网络协议传送。		47
AH	认证报头。源主机认证与数据完整性，但不保密。该协议通过 IPSec 远程网关设置为主动模式用于认证。		51
ESP	封装安全负载。手动密钥与 AutoKE VPN 通道在加密数据通信中使用该服务。		50
AOL	AOL 即时信息协议。	tcp	5190-5194
BGP	边界网关协议路由协议。BGP 是内部/外部路由协议。	tcp	179
DHCP	动态主机配置协议是从 DHCP 服务器到主机分配网络地址并提供配置参数。	udp	67
DNS	网域名称服务将域名转换为 IP 地址。	tcp	53
		udp	53
FINGER	提供有关用户信息的网络服务。	tcp	79
FTP	传输文件。	tcp	21
FTP_GET	上传文件。	tcp	21
FTP_GET	下载文件。	tcp	21
GOPHER	Gopher 通讯服务。Gopher 编排并以文件分级结构列表显示 Internet 服务器内容。	tcp	70
H323	H.323 多媒体协议。H.323 是国际电信联盟通过的协议标准定义视听会议数据是如何通过网络传输的。	tcp	1720，1503
HTTP	HTTP 是万维网以网页的形式进行数据传输的协议。	tcp	80
HTTPS	安全套接字层（SSL）服务的 HTTP 是基于 web 服务器的安全数据通讯。	tcp	443

服务名称	描述	协议	端口
IKE	IKE 是用来使用 IPSEC 的 ISAKMP 获得原始认证密钥的协议。	udp	500
IMAP	互联网消息访问协议（IMAP）是用于接收邮件消息的。	tcp	143
Internet-Locator-Service	互联网定位协议包括 LDAP，用户定位服务和基 TLS/SSL 的 LDAP。	tcp	389
IRC	互联网聊天中继允许用户连接到互联网并加入聊天组。	tcp	6660-6669
L2TP	L2TP 是一个用于远程访问的基于 PPP 的通道协议。	tcp	1701
LDAP	轻型目录访问协议是用于访问信息目录的一组协议。	tcp	389
NetMeeting	网络会议允许用户将互联网作为传输介质进 行远程电话会议。	tcp	1720
NFS	网络文件系统允许网络用户访问存贮在不同类型的计算机上的共享文件。	tcp	111，2049
NNTP	网络新闻传输协议是一个用于张贴发布和接收 USENET 消息的协议。	tcp	119
NTP	网络时间协议用于将计算机的时钟与时间服务器同步。	tcp	123
OSPF	开放最短路径优先路由协议。OSPF 是一个公共连接状态路由协议。		89
PC-Anywhere	PC-Anywhere 是远程控制域文件传输协议。	udp	5632
ICMP_ANY	Internet 控制消息协议是主机域网关(Internet）之间消息控制域报错协议。		
PING	用于测试与其它设备连接的 ICMP 回应请求与回复。	icmp	8
TIMESTAMP	ICMP 时间戳请求信息。	icmp	13
INFO_REQU EST	ICMP 信息请求信息。	icmp	15
INFO_ADDR ESS	ICMP 地址掩码请求信息。	icmp	17
POP3	邮局协议是从 POP3 服务器下载邮件的电子邮件协议。	tcp	110
PPTP	点对点通道协议是允许公司基于公网通过私网通道扩展网络的协议。	tcp	1723

服务名称	描述	协议	端口
QUAKE	用于流行游戏 QUAKE 多人游戏的连接。	udp	26000， 27000， 27910， 27960
RAUDIO	串流多媒体数据流。	udp	7070
RLOGIN	用于登录远程服务器的服务。	tcp	513
SAMBA	Samba 允许微软 Windows 用户从启动 TCP/IP 的主机上使用文件与打印服务。	tcp	139
RIP	路由信息协议是一项通用距离向量路由协议。	udp	520
SIP	会话发起协议是用来定义视听会议数据如何通过网络传输的。	udp	5060
SIP-MSNmess enger	是微软出品的 MSN 发起一个交互式可能为多媒体会话时使用的协议。		
SMTP	简单邮件传输协议用于在邮件服务器之间的邮件传输。	tcp	25
SNMP	简单网络管理协议是用于复杂网络管理的一套协议。	tcp	161-162
		udp	161-162
SSH	对计算机进行远程管理时使用的安全访问连接服务。	tcp	22
		udp	22
SYSLOG	进行远程日志记录的服务。	udp	514
TALK	支持两个或更多用户之间会话的协议。	udp	517-518
TCP	所有的 TCP 端口。	tcp	0-65535
TELNET	运行命令与远程计算机建立连接的服务。	tcp	23
TFTP	一般的文件传输协议；类似 FTP，简单文件的 传输协议但是不具备安全特性。	udp	69
UDP	所有的 UDP 端口。	udp	0-65535
UUCP	基本联网使用程序，是简单文件拷贝协议。	udp	540
VDOLIVE	用于 VDO Live 多媒体数据流通讯。	tcp	7000-70
WAIS	广域信息服务，internet 搜索协议。	tcp	210
WINFRAME	运行 windows NT 的计算机之间的 WinFrame 通讯。	tcp	1494
X-WINDOWS	X-Window 服务器与 X-Window 客户端之间的远程通讯。	tcp	6000-60

15.3 查看用户服务列表

如果 ZXSEC US 设备启动了虚拟域,需要对每个虚拟域配置单独的用户服务。在主菜单页面点击中点击虚拟域，可以查看虚拟域配置的用户服务。

如果您需要为预先定义服务列表中不包含的服务创建策略时，需要添加用户服务。

进入防火墙>服务>定制，可以查看用户服务列表。

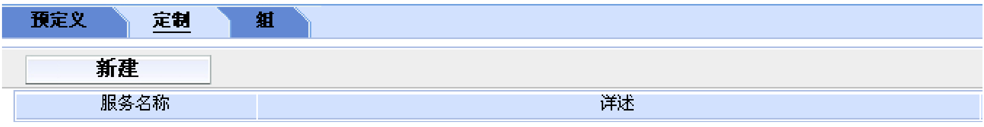


图15.3-1 用户服务列表

用户服务列表中的图标及其功能：

参数名称	参数说明
新建	选择协议，点击新建添加定制服务。
服务名称	用户服务名称。
详述	每项用户服务定义的协议与端口号。
删除图标	点击该图标，将服务条目从列表中删除。只有在地址组没有用于防火墙策略时才可以被删除。
编辑图标	点击编辑图标，编辑服务名称、协议类型、协议编号、编码、源端口以及目标端口项。

15.4 配置用户服务

配置防火墙策略的同时可以创建用户服务。点击服务项的下拉列表中点击“新建”。

添加用户 **TCP** 或 **UDP** 服务

1. 进入防火墙>服务>定制。
2. 将协议类型设置为 TCP/UDP。
3. 配置以下选项。

新建自定义服务

名称

协议 TCP/UDP

协议	源端口		目的端口	
	低级	高级	低级	高级
TCP	1	65535	0	0

添加

OK 取消

图15.4-1 **TCP** 与 **UDP** 用户服务选项

参数名称	参数说明
名称	TCP 或 UDP 用户服务的名称。
协议	将协议类型设置为：TCP/UDP。
协议	在协议项中分别选择 TCP 与 UDP。
源端口	输入低与高端口号码设定服务的源端口号范围。如果服务使用单个端口号码，在低端口与高端口域输入相同的端口号。缺省数值设定下允许使用任何源端口。
目的端口	输入低与高端口号码质点服务的目标端口号范围。如果服务使用单个端口号码，在低端口与高端口域输入相同的端口号。
添加	如果创建用户服务时需要不止一个端口范围。点击“添加”允许创建多个源与目标范围
删除图标	点击该图标从列表中删除条目。

根据您所定义的用户服务协议类型显示不同的选项。以下是服务选项：TCP，UDP，ICMP 或 IP。

添加用户 **ICMP** 服务

1. 进入防火墙>服务>定制。
2. 将协议类型设置为 ICMP。
3. 配置以下选项。

新建自定义服务

名称
协议 ICMP
类型 0
代码 1
OK 取消

图15.4-2 **ICMP** 用户服务选项

参数名称	参数说明
名称	ICMP 用户服务名称。
协议	选择您所添加服务的协议类型为 ICMP。
类型	输入该服务的 ICMP 协议号。
代码	如需要，输入 ICMP 代码值。

IP 用户服务选项

1. 进入防火墙>服务>定制。
2. 将协议类型设置为 ICMP。
3. 配置以下选项。

新建自定义服务

名称
协议 IP
协议号 6
OK 取消

图15.4-3 **IP** 用户协议选项

参数名称	参数说明
名称	IP 用户服务名称。
协议	选择您所添加服务的协议类型为 IP。
协议号	该服务的 IP 协议号。

15.5 查看服务组列表

如果 ZXSEC US 设备启动了虚拟域，需要对每个虚拟域配置单独的用户组服务。在主菜单页面点击中点击虚拟域，可以查看虚拟域配置的用户服务组。

为了便于添加防火墙策略，您可以创建服务组并将其添加在一个策略中允许或屏蔽对该组中服务的访问。服务组可以包含预先定义的服务与用户服务，或两者的任何结合。您不可以将一个服务组添加到其它的服务组中。

进入防火墙>服务>组，查看服务组列表。

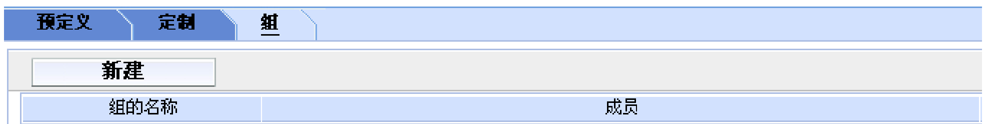


图15.5-1 服务组列表

服务组列表中的图标及其功能：

参数名称	参数说明
新建	点击新建添加服务组。
组的名称	服务组的名称。
成员	添加在服务组的服务。
删除图标	点击从列表中删除条目。只有在地址组没有用于防火墙策略时才可以被删除。
编辑图标	对组名称以及组成员进行编辑。

15.6 配置服务组

进入防火墙>服务>组，可将服务编排到服务组中。

创建或添加服务组时可以配置服务组选项。



图15.6-1 新建服务组列表

服务组具有以下选项。

参数名称	参数说明
服务组名称	输入地址组的名称。
可用服务	创建服务组时可用的服务。使用左右箭头在两个列表之间移动添加服务。
成员	服务列表。使用左右箭头在两个对话框之间移动服务。

第16章 防火墙时间表

16.1 概述

描述

设置时间表控制激活与中止策略的时间。您可以设置固定时间表或循环时间表。使用固定时间表创建一项策略在指定的时间段内生效。循环时间表每周进行一个循环。您可以使用循环时间表设置一项策略只在指定的一天中循环几次或一星期中某些天之内生效。

内容

16.2 查看单次时间表

如果 ZXSEC US 设备中启动了虚拟域设置，单次时间表需要对每个虚拟域单独配置。查看虚拟域的时间表需要从主菜单中选择虚拟域，然后进行查看。

您可是创建单次时间表指定的激活或中止一项策略的时间。例如，防火墙配置默认的策略允许任何时间下对全部服务的访问，您可以添加一个固定时间列表设置在假期时间内阻止到 internet 的任何连接。

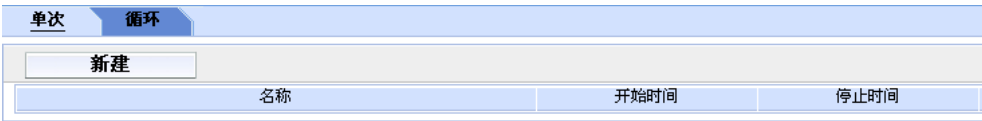


图16.2-1　单次时间表

单次时间列表中的图标以及其功能：

参数名称	参数说明
新建	点击新建添加固定时间表。
名称	单次时间表的名称。
开始时间	设置开始时间。

参数名称	参数说明
停止时间	设置停止时间。
删除图标	点击删除列表中的条目不是应用在防火墙策略中的时间列表条目才可以被删除。
编辑图标	点击编辑时间表。

16.3 配置单次时间表

在配置防火墙策略时，“时间表”选项的下拉菜单中点击“新建”可以创建时间表。进入“防火墙>时间表>单次”，可以配置时间表。

图16.3-1　单次时间表选项

单次时间表具有以下选项。

参数名称	参数说明
名称	输入固定时间表的名称。
开始时间	设置开始时间。
结束时间	设置结束时间。

将开始与结束时间设置为 00 表示设置策略整天都在激活状态。固定时间表运行的是 24 小时制。

16.4 查看循环时间表

如果 ZXSEC US 设备启动了虚拟域，需要对每个虚拟域配置单独的循环时间表。在主菜单页面点击中点击虚拟域，可以查看虚拟域配置的用户服务组。

您可以创建循环时间表指定一天中的循环次数或一周中的某些天激活或中止运行防火墙策略。例如，您可以通过创建循环时间表禁止在工作时间玩游戏。



注意：

如果您在创建循环时间列表时，结束时间的设定早于开始时间，那么将在设置的开始时间执行但是结束的时间将托延至接下来一天的设置的结束时间结束任务。您也可以使用该设置的这一特点创建循环时间列表在一天开始并在接下来的另一天结束。或可以将开始与结束设置为同一时间，这样循环时间表便可以运行 24 个小时。

单次 循环

新建

名称	工作日	开始时间	停止时间	
always	SMTWTFS	00:00	00:00	

图16.4-1 循环时间表

循环时间表中的图标以及其功能：

参数名称	参数说明
新建	点击新建添加循环时间表。
名称	循环时间表的名称。
工作日	循环时间表激活的时间（一周中每天英文名称大写首字母）。
开始时间	循环时间表的开始时间。
结束时间	循环时间表的结束时间。
删除图标	点击删除列表中的条目。不是应用在防火墙策略中的时间列表条目才可以被删除。
编辑图标	点击编辑循环时间表。

16.5 配置循环时间表

在配置防火墙策略时，“时间表”选项的下拉菜单中点击“新建”可以创建时间表。

进入“防火墙>时间表>循环”，可以配置循环时间表。

图16.5-1　循环时间表选项

循环时间表中有以下选项：

参数名称	参数说明
名称	输入循环时间表的名称。
工作日	选择激活循环时间表的时间（一周中的某天）。
开始时间	设置循环时间表的开始时间。
停止时间	设置循环时间表的停止的时间。

循环时间表采用的 24 小时制。

第17章 防火墙虚拟 IP 地址配置

17.1 概述

描述

本章节是有关 ZXSEC US 虚拟 IP 地址、IP 地址池以及配置在防火墙策略中配置使用等功能。

内容

17.2 虚拟 IP 地址

使用虚拟 IP 能够访问源网络中被 NAT（network adress translation：网络地址转换）安全策略隐藏的目标网络的 IP 地址。虚拟 IP 使用代理 ARP，ZXSEC US 设备可以对实际安装在另一个网络中服务器发出的 ARP 请求作出响应。代理 ARP 在 RFC1027 中进行了定义。

例如，您可以在外部网络 ZXSEC US 设备接口添加一个虚拟 IP 地址，那么外部接口就可以对实际上与 DMZ 或内部网络中服务器连接的用户发出的请求作出回应。

通过 ZXSEC US 设备，虚拟 IP 是如何实现映射的

以使用静态 NAT 虚拟 IP 地址允许到 ZXSEC US 设备设置保护私网中的服务器进行访问为例，回归到这个例子应用的基础无非是涉及了三个部分，如下图所示，

私网中的 web 服务器，互联网中浏览计算机以及与这两个网络连接的 ZXSEC US 设备。

一个用户计算机试图访问服务器。用户计算机发送数据包，ZXSEC US 设备接收到这些数据包。数据包的地址将被隐藏并重新映射，然后被转发到私网的服务器。



图17.2-1　单个静态 NAT 虚拟 IP 地址使用示例

从用户发送数据包的源 IP 地址与目标地址分别是 192.168.37.55 与 192.168.37.4。ZXSEC US 在外部接口接收这些数据包。虚拟 IP 设置将 192.168.37.4 映射为 10.10.10.2。因此数据包的地址发生更改。源地址变为 10.10.10.2，目标地址变为 10.10.10.42。ZXSEC US 设备将在防火墙通信会话中记录该地址的转换。数据包将被转发到服务器计算机。



图17.2-2　从用户到服务器的网络地址转换过程汇中数据包地址的更改

需要说明的是，用户计算机发出的数据包地址在服务器接收到该数据包时并不显示。ZXSEC US 设备对网络地址更改后，并不影响用户计算机网络。而服务器网络并不知道其它网络的连接。服务器所获知的全部信息是，所有的通信会话都是来自 ZXSEC US 设备的。

服务器对用户设备的回应，操作步骤如果用户计算机发送数据包到服务器一样，只是数据返回的方向不同。服务器发送回应数据包，该数据包的源 IP 地址与目标 IP 地址分别是 10.10.10.42 与 10.10.10.2。ZXSEC US 设备在内部接口接收这些数据包。这一次，防火墙会话表条目将用来决定目标地址的转换。

在这个例子中，源地址与目标地址分别被更改为 192.168.37.4 与 192.168.37.55，回应数据包到达用户计算机。

从以上示例中可以看出，服务器与用户设备均不知道对方的存在，双方都是将 ZXSEC US 设备作为数据包到达的终点。ZXSEC US 设备从中实现了地址的转换并不影响双方的通信。



图17.2-3　从服务器将回应数据包发送到用户时应用 NAT（地址转换）后发生的映射情况



注意：

运行于透明模式下的 ZXSEC US 设备不能够应用虚拟 IP 地址功能。

一个虚拟 IP 地址可以是与 ZXSEC US 设备接口捆绑的单个 IP 地址或一个 IP 地址群。当您应用虚拟 IP 地址功能，将一个 IP 地址或 IP 地址群与 ZXSEC US 设备接口绑定后，该接口将对 ARP 请求作出响应。

如果在创建防火墙策略时没有选中 NAT 功能框，那么该策略将执行目标网络地址转换（DNAT）。DNAT 从外部网络接收将要到达具体目标 IP 地址的数据包，并将该数据包的目标地址转换映射到另外一个隐藏网络的 IP 地址，然后将数据包通过 ZXSEC US 设备转发到隐藏的目标网络。与上述的例子不同的是数据包的源地址没有被转换。在隐藏目标网络中，数据包达到其最终的目的地。

虚拟 IP 范围可以是任何长度的 IP，并可以将地址转换为不同子网的地址。虚拟 IP 的设置有以下几点限制：

1. 映射 IP 地址不可以设置为 0.0.0.0 或 255.255.255.255。
2. 如果虚拟 IP 的类型为静态 NAT 并且映射到一个 IP 地址范围，外部 IP 地址不可以是 0.0.0.0。只有当虚拟 IP 类型设置为负载平衡，并且静态 NAT 虚拟 IP 映射到单个的 IP 地址时，才支持将外部 IP 设置为 0.0.0.0.。

3. 端口映射是将外部端口号的范围转换为一个内部端口号的范围。这两个端口号范围间的端口数目必须相等。因此，外部端口号不应该进行设置，那么其范围设置上限不能超过 65535。例如，以一个端口 65530 开始的外部范围来映射一个有 20 个端口的内部范围，是无效的，因为最大端口号会达到 65550。
4. 设置为“端口转发”时，外部 IP 范围不能够包括任何接口 IP 地址。
5. 映射的 IP 范围不必包括任何接口 IP 地址。
6. 虚拟 IP 名称不能与任何地址或地址组的名称相同。
7. 不允许复制条目或范围重叠。

除了将 IP 地址或 IP 地址范围与接口绑定外，虚拟 IP 中还包括接口映射 IP 地址与范围的所有消息，该接口与发出实际 IP 地址或 IP 地址范围的接口连接的是同一个网络。

您可以设置不同类型的虚拟 IP，每种类型都能够用于不同的 DNAT 变量。参数信息如下表所示。

参数信息

参数名称	参数说明
静态 NAT	用于将源网络中的地址转换成目的网络中的隐藏的地址。静态 NAT 将返回的数据包的源地址转换为源网络中的地址。 静态 NAT 虚拟 IP 使用的是单对单的映射。一个外部 IP 地址映射到单个的 IP 地址。在源地址范围内给定的 IP 地址总是映射到目标地址范围内相同的 IP 地址。
静态端口转发	静态 NAT 端口转发是将一个网络中单个的 IP 地址或 IP 地址范围以及单个的端口或端口范围映射到另一个网络中不同的单个的 IP 地址或 IP 地址范围以及单个端口或端口范围。 静态 NAT 端口转发也简称为端口转发。静态 NAT 端口转发虚拟 IP 是一对一的端口映射。外部 IP 地址范围以及外部端口号分别映射到对应的 IP 地址与端口号。端口转发虚拟 IP 可以配置 ZXSEC US 设备应用端口地址转换（PAT）。
负载平衡端口转发	负载平衡也称为动态端口转发。负载平衡虚拟 IP 可以将一个网络中的单个 IP 映射到其它网络中一个 IP 地址范围。 负载平衡应用了一对多的映射原理。负载平衡算法是从一个 IP 地址范围中分配目标 IP 地址以保证流量的均衡。 负载平衡端口转发是将一个网络中的单个 IP 地址与端口号映射到另一个网络中 IP 地址与端口号范围。 负载平衡端口转发是应用一对多负载平衡算法从 IP 地址范围中

参数名称	参数说明
	分配目标 IP 地址以保证流量的均衡，并从目标端口范围分配目标端口。
动态虚拟 IP	如果您将外部虚拟 IP 设置为 0.0.0.0，您可以创建动态 IP 地址将任何 IP 地址映射到 IP 地址或 IP 地址范围。
动态端口转发	类似于端口转发，动态端口转发可以将任何地址与源网络中具体的端口号转换为一个隐藏的地址或目标网络中不同的端口号。 您必须在 NAT 防火墙策略中添加虚拟 IP 以便执行虚拟 IP 映射。添加防火墙策略将外部网络地址映射到内部网络，您在内部防火墙策略中添加一个外部接口地址并在策略中目标地址字段中添加一个虚拟 IP。 例如，内部网络中作为 web 服务器的设备的私有 IP 地址是 10.10.10.42。web 服务器从互联网数据包获得数据包必须具有一个外部地址。在防火墙配置中添加一个虚拟 IP，将 web 服务器的外部 IP 与内部 IP 发生映射。在内部防火墙策略中添加外部地址并将目标地址设置为虚拟 IP 地址，允许 web 服务器到互联网的连接。

17.3 查看虚拟 IP 地址列表

进入“防火墙>虚拟 IP>虚拟 IP”，查看虚拟 IP 列表。

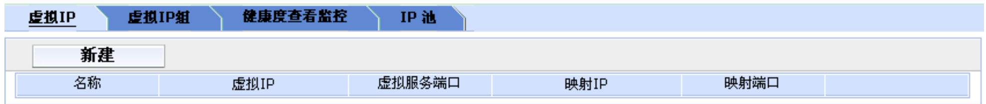


图17.3-1　虚拟 IP 列表

虚拟 IP 列表中包含的图标及其功能如下表所示。

参数信息

参数名称	参数说明
新建	点击新建添加虚拟 IP。
名称	虚拟 IP 的名称。
虚拟 IP	与目标网络地址相映射的外部 IP 地址或 IP 地址范围。
服务端口	外部端口号或端口号范围。 服务端口被包括在端口转发虚拟 IP 中。
映射 IP/IP 地址范围	映射到目标网络中 IP 地址或 IP 地址范围。
映射端口	所映射的端口号或端口范围。端口转发虚拟 IP 支持端口映射。
删除图标	将虚拟 IP 从列表中删除。 只有在防火墙策略中不使用虚拟 IP 是该删除图标才可用。
编辑图标	编辑虚拟 IP 设置包括更改任何虚拟 IP 选项以及虚拟 IP 名称。

17.4 配置虚拟 IP 地址

进入“防火墙>虚拟 IP>虚拟 IP”并点击“新建”添加虚拟 IP 列表。在该菜单项下，点击“编辑”图标，可以编辑虚拟 IP 选项。

虚拟 IP 具有以下选项如下表所示。

参数信息

参数名称	参数说明
名称	虚拟 IP 的名称。输入虚拟 IP 的名称。地址，地址组与虚拟 IP 必须具有单独的名称避免在配置防火墙策略中发生混乱。
外部接口	从列表中选择虚拟 IP 外部接口。外部接口与源网络连接并接收数据包将其转发到目标网络。您可以设置为任何 ZXSEC US 接口，VLAN 子接口及 VPN 接口。
类型	选择“静态 NAT”或“负载平衡”。 输入与目的网络中地址相映射的外部 IP 地址。将外部 IP 地址设置为 0.0.0.0.，配置动态 IP 接收任何 IP 地址的连接。
映射到 IP 地址/范围	对于静态 NAT 动态虚拟 IP，您只能添加一个映射 IP 地址。对于负载平和动态虚拟 IP，您可以指定单个的映射地址或地址范围。 输入映射到外部 IP 地址的目标网络中真实的 IP 地址。您也可以输入一个地址范围将数据包转发到目标网络中多个 IP 地址。 对于静态 NAT 虚拟 IP，如果您添加一个映射 IP 地址范围，ZXSEC US 设备计算出外部 IP 地址范围并将该地址范围添加到外部 IP 地址/范围字段。
方式	如果您设置“服务器负载平衡”，您可以选择以下的负载平衡方式。 静态：流量平均在所有服务器之间分配，不需要额外的服务器。 轮询：直接请求下一台的服务器，无论各个服务器的反间或连接量如何，都一视同仁。避免失效的服务器或没有回应的服务器。需要单独的服务器。 权重：设置权重值高的服务器将接收大部分的连接。添加服务器时可以设置服务器的权重值。
端口转发	点击添加端口转发虚拟 IP。
协议	输入转发数据包时使用的协议（TCP 或 UDP）。
外部服务端口	输入在配置端口转发时外部服务端口号。
映射到端口	外部端口号映射到目标网络中的端口号。 您也可以一个端口号范围将数据包转发到目标网络中多个端口。对于静态 NAT 虚拟 IP，如果您添加一个端口范围的映射，ZXSEC US 设备将计算出外部端口号范围并将其添加到外部服务端口字段。
真实服务器	如果您对 VIP 流量设置“服务器负载平衡”，输入真实服务器的

参数名称	参数说明
	IP 地址。至少需要一个 IP 地址，最多可以添加 8 个地址。 输入服务器 IP 地址时，点击添加真实服务器并输入以下信息。 IP：输入服务器的 IP 地址。 端口：如果启动端口转发，输入外部端口映射到的目标网络中的端口号。 失效间隔：连接在被丢弃之前保持闲置的时间间隔。设置范围为 10 到 255 秒。 唤醒间隔：放弃服务器检测之前的间隔时间。设置范围为 10 到 255 秒。 权重：设置服务器的权重值。值越高，处理的流量比例越多。设置范围为 1 到 255。 健康度：启动该选项，在转发会话之前使用 ping 命令检测服务器的状态。

17.4.1 对单个 IP 地址添加静态 NAT 虚拟 IP

互联网中 IP 地址为 192.168.3.7 映射到私网中的地址为 10.10.10.42。互联网中试图与 192.168.37.4 的地址被转换并以 10.10.10.42 被发送。位于互联网中的计算机设备不会注意这样的地址转换，看到的具有地址为 192.168.37.4 的单个设备而不是与私网连接的 ZXSEC US 设备。

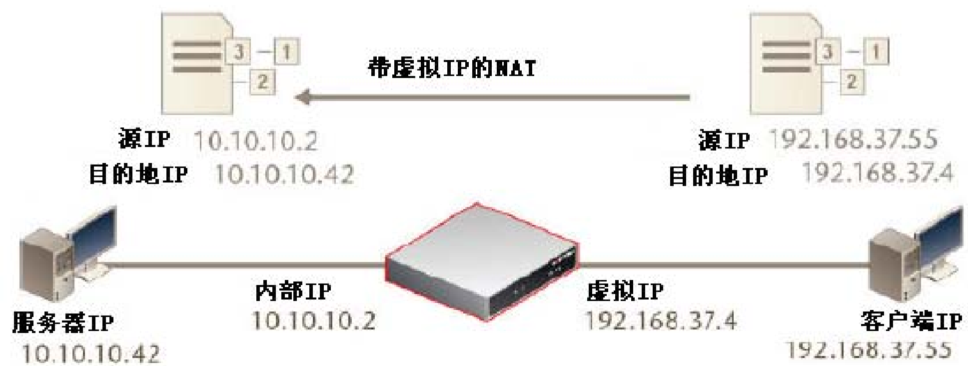


图17.4-1 单个 IP 地址的静态 NAT 虚拟 IP 设置示例

对单个虚拟 IP 添加静态 NAT 虚拟 IP 地址：

1. 进入防火墙>虚拟 IP>虚拟 IP。
2. 点击“新建”。

3. 使用以下步骤添加虚拟 IP，允许互联网中的用户连接到 DMZ 网络中的 web 服务器。在以下我们所举的例子中，ZXSEC US 设备的外部接口与互联网连接以及通过 dmz1 接口与 DMZ 网络连接。

参数信息

参数名称	参数说明
名称	simple_static_NAT
外部接口	external
类型	静态 NAT
外部 IP	Web 服务器的互联网 IP 地址。
地址/范围	外部 IP 地址必须是从 web 服务器 ISP 获得的静态 IP 地址。该地址必须是不被其他主机使用唯一性的地址，该地址也不能应用虚拟 IP 的外部接口地址相同。但是，外部 IP 地址必须路由到所选的接口。虚拟 IP 地址与外部 IP 地址可以处于不同的子网。当您设置虚拟 IP 时，外部接口将对 ARP 请求作出回应。
映射到 IP/IP 地址范围	内部网络中服务器的 IP 地址。因为只有一个 IP 地址，第二个地址栏保留为空。

新建虚拟IP映射

名称

外部接口 port2

类型 静态NAT 服务器负载均衡

外部的IP地址或范围 0.0.0.0

影射的IP地址或范围 0.0.0.0

端口转发

确定 取消

图17.4-2 单个 IP 地址的静态 NAT 虚拟 IP 设置

4. 点击“OK”确认。

将对单个 IP 地址设置的静态 NAT 虚拟 IP 地址添加在防火墙策略中

将外部接口添加到 dmz1 防火墙策略中应用虚拟 IP 设置，以便当互联网中的用户试图连接到 web 服务器，IP 数据包能够通过 ZXSEC US 设备从外部接口到达 dmz1 接口。虚拟 IP 将这些数据包的目标地址从外部 IP 转换为 web 服务器所处的 DMZ 网络 IP 地址。

1. 进入防火墙>策略。

2. 点击“新建”。

3. 配置以下防火墙策略。

参数信息

参数名称	参数说明
源接口/区域	external
源地址名称	全部（或一个具体的 IP 地址）
目标接口/区域	dmz1
目标地址名称	simple_static_NAT
时间表	循环
服务	HTTP
动作	ACCEPT（接受）

4. 点击“NAT”。

5. 点击“OK”确认。

17.4.2 对一个 IP 地址范围添加静态 NAT 虚拟 IP 设置

互联网中 IP 地址范围为 192.168.37.4 到 192.168.37.6 映射到私网中 10.10.10.42 到 10.10.123.44。互联网中计算机发出的数据包与 192.168.37.4 的通信过程中地址将被转换并由 ZXSEC US 设备发送到地址为 10.10.10.42。简而言之，到达目的地 192.168.37.5 的数据包地址被转换并被发送到 10.10.10.43；到达目的地 192.168.37.5 的数据包地址被转换并为发送到 10.10.10.44。在互联网中的计算机设备并不能察觉地址转换，所获知的只是三台设备具有各自不同的 IP 地址而不是与私网连接的 ZXSEC US 设备。

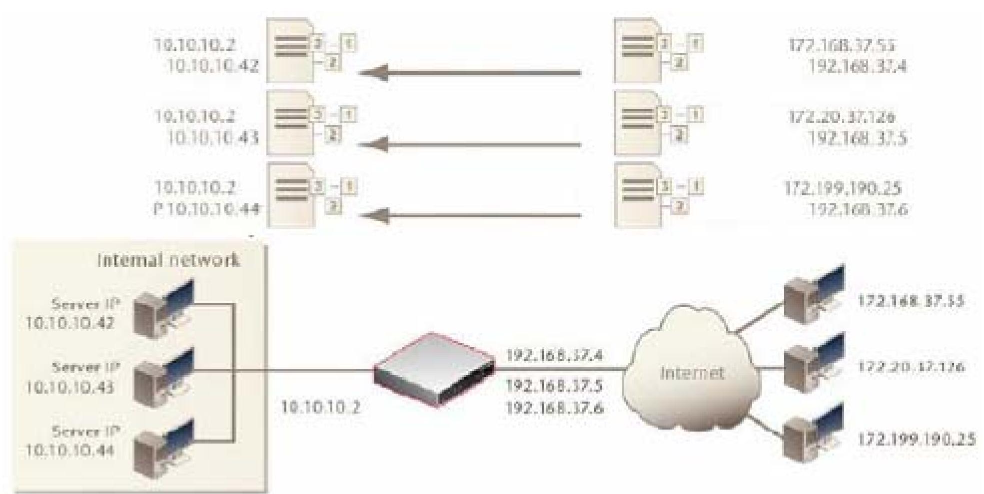


图17.4-3 对一个 IP 地址范围配置静态 NAT 虚拟 IP 设置示例

对 IP 地址范围添加静态 NAT 虚拟 IP 设置：

1. 进入“防火墙>虚拟 IP>虚拟 IP”。

2. 点击“新建”。

3. 使用以下步骤添加虚拟 IP，允许互联网中的用户分别连接到 DMZ 网络中的三台 web 服务器。在我们的示例中，ZXSEC US 设备的外部接口连接到互联网，dmz1 接口与 DMZ 网络连接。

参数信息

参数名称	参数说明
名称	static_NAT_range
外部接口	external
类型	静态 NAT
外部 IP	Web 服务器的互联网 IP 地址。
地址/范围	外部 IP 地址必须是从 web 服务器 ISP 获得的静态 IP 地址。该地址必须是不被其他主机使用唯一性的地址，该地址也不能应用虚拟 IP 的外部接口地址相同。但是，外部 IP 地址必须路由到所选的接口。虚拟 IP 地址与外部 IP 地址可以处于不同的子网。当您设置虚拟 IP 时，外部接口将对 ARP 请求作出回应。
映射到 IP/IP 地址范围	内部网络中服务器的 IP 地址范围。通过在第一个字段输入起始 IP 地址在第二个字段输入结束的 IP 地址来定义一个 IP 地址范围。

新建虚拟IP映射

名称 static_NAT_range
外部接口 port2
类型 静态NAT 服务器负载均衡
外部的IP地址或范围 0.0.0.0
影射的IP地址或范围 0.0.0.0
端口转发
协议 TCP UDP
外部服务端口
映射到端口
HTTP多路传输
保留用户IP
确定 取消

图17.4-4 虚拟 IP 选项；IP 地址范围的静态 NAT 虚拟 IP 设置

4. 点击“OK”确认。

将设置了静态 NAT 虚拟 IP 的 IP 地址范围添加到防火墙策略中

将 wan1 接口应用虚拟 IP 设置添加 dmz1 防火墙策略中，那么当位于互联网中的用户试图与服务器 IP 地址连接时，数据包从外部接口通过 ZXSEC US 设备到达 dmz1 接口。虚拟 IP 设置将这些数据包的目的地地址从外部 IP 转换为服务器所处的 DMZ 网络的 IP 地址。

1. 进入防火墙>策略，并点击“新建”。
2. 配置防火墙策略。

参数信息

参数名称	参数说明
源接口/区域	external
源地址名称	全部（或一个具体的 IP 地址）
目标接口/区域	dmz1
目标地址名称	static_NAT_range
时间表	循环
服务	HTTP
动作	ACCEPT（接受）

3. 点击“NAT”。
4. 点击 OK 确认。

17.4.3 对单个 IP 地址与端口设置静态 NAT 端口转发

互联网中 IP 地址 192.168.37.4，端口 80 映射到私网中为 10.10.10.42 以及端口 8000 的连接。从互联网试图与 192.168.37.4.端口 80 建立连接时地址被转换并通过 ZXSEC US 设备发送到 10.10.10.10.42.端口 8000。互联网中的计算机设备并不会对该转换有所反映，认为连接的是地址 192.168.37.4 与端口 80 的设备而不是与私网连接的 ZXSEC US 设备。

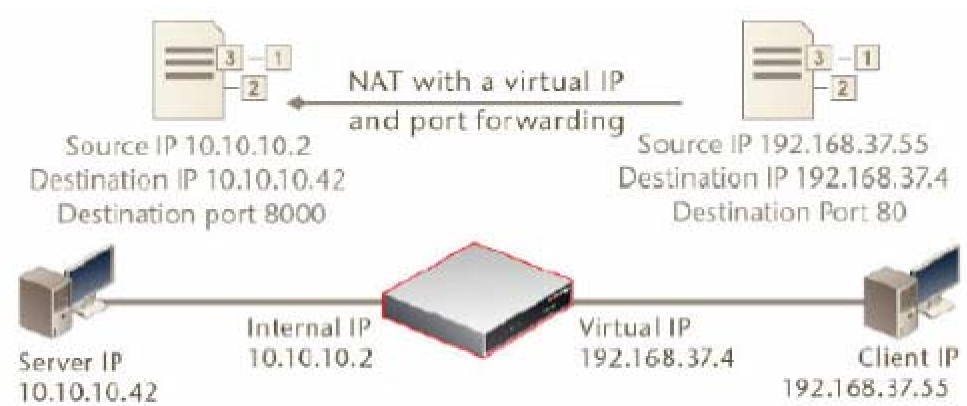


图17.4-5　对单个 IP 地址与端口配置静态 NAT 虚拟 IP 设置示例

对单个 IP 地址与单个端口配置静态 NAT 虚拟 IP 设置

1. 进入“防火墙>虚拟 IP>虚拟 IP”。
2. 点击“新建”。
3. 使用以下步骤添加虚拟 IP，允许互联网中的用户连接到 DMZ 网络中的 web 服务器。在以下我们所举的例子中，ZXSEC US 设备的外部接口与互联网连接以及通过 dmz1 接口与 DMZ 网络连接。

参数信息

参数名称	参数说明
名称	Port_fwd_NAT_VIP
外部接口	external
类型	静态 NAT
外部 IP	Web 服务器的互联网 IP 地址。
地址/范围	web 服务器的互联网 IP 地址。外部 IP 地址必须是从 web 服务器 ISP 获得的静态 IP 地址。该地址必须是不被其他主机使用唯一性的地址，该地址也不能应用虚拟 IP 的外部接口地址相同。但是，外部 IP 地址必须路由到所选的接口。虚拟 IP 地址与外部 IP 地址可以处于不同的子网。当您设置虚拟 IP 时，外部接口将对 ARP 请求作出回应。
映射到 IP/IP 地址范围	内部网络中服务器的 IP 地址范围。只填写一个 IP 地址栏，保持第二个地址栏为空。
端口转发	选中该功能框。
协议	设置为 TCP。
外部服务端口	与互联网发生通信使用的端口号。对于 web 服务器，一般通常使用的端口号为 80。
映射到端口	web 服务器接收流量使用的端口。只需要使用一个端口，另

参数名称	参数说明
	一个端口号保留为空。

编辑虚拟IP映射

名称 port

外部接口 port2

类型 静态NAT 服务器负载均衡

外部的IP地址或范围 192.168.37.4

影射的IP地址或范围 10.10.10.42

端口转发

确定 取消

图17.4-6　虚拟 IP 选项；对单个 IP 地址与端口设置静态 NAT 端口转发

4. 点击“OK”确认。

将设置了静态 NAT 虚拟 IP 的单个 IP 地址与端口添加到防火墙策略中

将 wan1 接口应用虚拟 IP 设置添加 dmz1 防火墙策略中，那么当位于互联网中的用户试图与服务器 IP 地址连接时，数据包从 wan1 接口通过 ZXSEC US 设备到达 dmz1 接口。虚拟 IP 设置将这些数据包的目的地地址从外部 IP 转换为服务器所处的 DMZ 网络的 IP 地址。

1. 进入防火墙>策略。
2. 点击“新建”。
3. 配置防火墙策略。

参数信息

参数名称	参数说明
源接口/区域	external
源地址名称	全部（或一个具体的 IP 地址）
目标接口/区域	dmz1
目标地址名称	Port_fwd_NAT_VIP
时间表	循环。
服务	HTTP
动作	ACCEPT（接受）

4. 点击“NAT”。
5. 点击 OK 确认。

17.4.4 对一个 IP 地址范围与端口范围设置静态 NAT 端口转发设置

互联网中地址范围为 192.168.37.4 到 192.168.37.7 的端口范围为 80 到 83 映射到私网的地址与端口范围分别为 10.10.10.42 到 10.10.10.44 以及端口 8000 到 8003。互联网中计算机发出的数据包与 192.168.37.5.端口号为 82 的通信过程中地址将被转换并由 ZXSEC US 设备发送到地址为 10.10.10.43.端口 8002。在互联网中的计算机设备并不能察觉地址转换，所获知的只是 IP 地址为 192.168.37.5 而不是与私网连接的 ZXSEC US 设备。

1. 进入防火墙>虚拟 IP>虚拟 IP。
2. 点击“新建”。
3. 使用以下步骤添加虚拟 IP，允许互联网中的用户连接到 DMZ 网络中的 web 服务器。在以下我们所举的例子中，ZXSEC US 设备的 wan1 接口与互联网连接以及通过 dmz1 接口与 DMZ 网络连接。

参数信息

参数名称	参数说明
名称	Port_fwd_NAT_VIP
外部接口	external
类型	静态 NAT
外部 IP	Web 服务器的互联网 IP 地址。
地址/范围	web 服务器的互联网 IP 地址。外部 IP 地址必须是从 web 服务器 ISP 获得的静态 IP 地址。该地址必须是不被其他主机使用唯一性的地址，该地址也不能应用虚拟 IP 的外部接口地址相同。但是，外部 IP 地址必须路由到所选的接口。虚拟 IP 地址与外部 IP 地址可以处于不同的子网。当您设置虚拟 IP 时，外部接口将对 ARP 请求作出回应。
映射到 IP/IP 地址范围	内部网络中服务器的 IP 地址范围。通过在第一个字段输入起始 IP 地址在第二个字段输入结束的 IP 地址来定义一个 IP 地址范围。
协议	设置为 TCP。
外部服务端口	与互联网发生通信使用的端口号。对于 web 服务器，一般通常使用的端口号为 80。
映射到端口	web 服务器接收流量使用的端口。通过在第一个字段输入起始 IP 地址在第二个字段输入结束的 IP 地址来定义一个 IP 地址范围。因为只有一个端口，保留第二个端口为空。

4. 击“NAT”。

5. 点击 OK 确认。

将设置了静态 NAT 虚拟 IP 转发的 IP 地址范围与端口范围添加到防火墙策略中。

将应用虚拟 IP 的外部接口（external）设置添加 dmz1 防火墙策略中，那么当位于互联网中的用户试图与服务器 IP 地址连接时，数据包从外部接口通过 ZXSEC US 设备到达 dmz1 接口。虚拟 IP 设置将这些数据包的目的地地址从外部 IP 转换为服务器所处的 DMZ 网络的 IP 地址。

1. 进入防火墙>策略，并点击“新建”。

2. 配置防火墙策略。

参数信息

参数名称	参数说明
源接口/区域	external
源地址名称	全部（或一个具体的 IP 地址）
目标接口/区域	dmz1
目标地址名称	Port_fwd_NAT_VIP_port_range
时间表	循环。
服务	HTTP
动作	ACCEPT（接受）

3. 点击“NAT”。

4. 点击 OK 确认。

17.4.5 对一个 IP 地址范围添加负载平衡虚拟 IP 设置

示例，互联网中 IP 地址为 192.168.37.4 映射到位于 ZXSEC US 设备之后的服务器中地址为 10.10.123.42，10.10.123.43 与 10.10.123.44。IP 地址映射是由 ZXSEC US 设备的负载平衡算法决定的。互联网中试图与 192.168.37.4 地址通信的请求将被转换并由 ZXSEC US 设备发送到 10.10.123.42，10.10.123.43 与 10.10.123.44。互联网中的计算机设备不会对此转换产生任何察觉并且只能访问地址为 192.168.37.4 的计算机设备，而不是私网中的 ZXSEC US 设备。



注意：

服务器负载平衡将一个网络中的单个 IP 最多可以映射到其他网络中真实服务器上的八个 IP 地址。使用该功能时需要至少添加一个真实的地址。

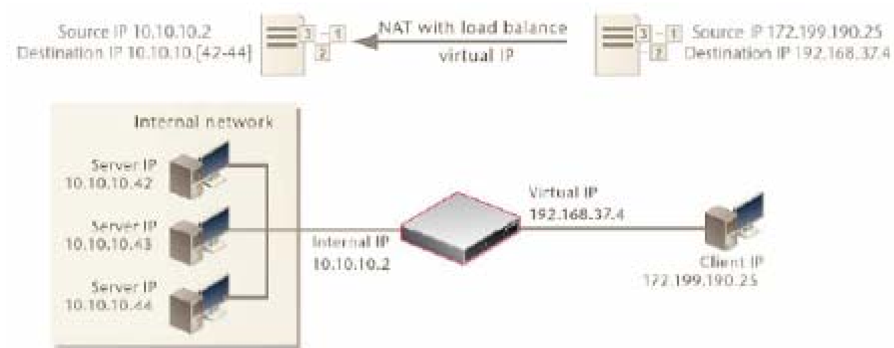


图17.4-7 服务器负载平衡虚拟 IP 地址

添加服务器负载平衡虚拟 IP 地址。

1. 进入“防火墙>虚拟 IP>虚拟 IP”。
2. 点击“新建”。
3. 使用以下步骤添加虚拟 IP，允许互联网中的用户连接到 DMZ 网络中的 web 服务器。在以下我们所举的例子中，ZXSEC US 设备的外部接口与互联网连接以及通过 dmz1 接口与 DMZ 网络连接。

参数信息

参数名称	参数说明
名称	Load_Bal_VIP
外部接口	external
类型	负载平衡
外部 IP	Web 服务器的互联网 IP 地址。
地址/范围	web 服务器的互联网 IP 地址。外部 IP 地址必须是从 web 服务器 ISP 获得的静态 IP 地址。该地址必须是不被其他主机使用唯一性的地址，该地址也不能应用虚拟 IP 的外部接口地址相同。但是，外部 IP 地址必须路由到所选的接口。虚拟 IP 地址与外部 IP 地址可以处于不同的子网。当您设置虚拟 IP 时，外部接口将对 ARP 请求作出回应。
映射到 IP/IP 地址范围	内部网络中服务器的 IP 地址范围。通过在第一个字段输入起始 IP 地址在第二个字段输入结束的 IP 地址来定义一个 IP 地址范围。
方式	设置为 TCP。设置负载平衡的方式。详细信息，参加“配置虚拟 IP”。
真实服务器	如果您对 VIP 类型设置服务器负载平衡，输入真实服务器的 IP 地址。有关真实服务器的详细信息，参见“配置虚拟 IP”。

新建虚拟IP映射
名称
外部接口 port2
类型 静态NAT 服务器负载均衡
外部的IP地址 0.0.0.0
方式 静态
端口转发
真实服务器
IP 端口 权重 健康度检查 监控器
添加
确定 取消

图17.4-8　虚拟 IP 选项；负载平衡虚拟 IP 设置

4.　点击 OK 确认。

将设置了负载平衡虚拟 IP 的 IP 地址范围添加到防火墙策略中。

将外部接口应用虚拟 IP 设置添加 dmz1 防火墙策略中，那么当位于互联网中的用户试图与服务器 IP 地址连接时，数据包从 wan1 接口通过 ZXSEC US 设备到达 dmz1 接口。虚拟 IP 设置将这些数据包的目的地地址从外部 IP 转换为服务器所处的 DMZ 网络的 IP 地址。

1.　进入防火墙>策略，并点击“新建”。

2.　配置防火墙策略。

参数信息

参数名称	参数说明
源接口/区域	external
源地址名称	全部（或一个具体的 IP 地址）
目标接口/区域	dmz1
目标地址名称	server_load_Bal_VIP
时间表	循环。
服务	HTTP
动作	ACCEPT（接受）

3.　点击“NAT”。

4.　点击 OK 确认。

17.4.6 对一个 IP 地址范围与端口范围配置负载平衡端口转发虚拟 IP 设置

从 Internet 到 192.168.37.4 的连接，在私有网络上被映射为到 10.10.10.42 到 10.10.10.44 地址段的连接。IP 地址映射是由 ZXSEC US 设备的负载平衡运算法则

决定的。地址 192.168.3.4 的端口 80 到 83 依次映射为端口 8000 到 8003。在互联网中的计算机设备并不能察觉地址转换，所获知的只是 IP 地址为 192.168.37.5 而不是与私网连接的 ZXSEC US 设备。

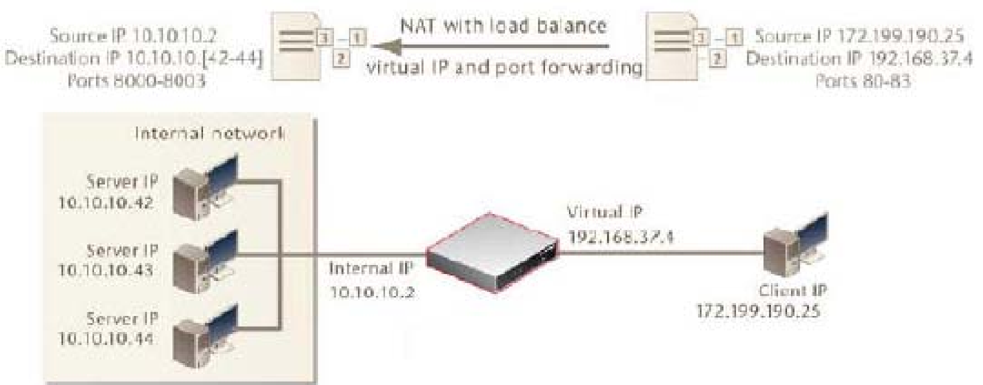


图17.4-9　对一个 IP 地址与端口范围配置负载平衡虚拟 IP 设置示例

添加服务器负载平衡端口转发虚拟 IP

1. 进入“防火墙>虚拟 IP>虚拟 IP”。
2. 点击“新建”。
3. 使用以下步骤添加虚拟 IP，允许互联网中的用户连接到 DMZ 网络中的 web 服务器。在以下我们所举的例子中，ZXSEC US 设备的外部接口与互联网连接以及通过 dmz1 接口与 DMZ 网络连接。

参数信息

参数名称	参数说明
名称	Load_Bal_VIP_port_forward
外部接口	external
类型	负载平衡
外部 IP	Web 服务器的互联网 IP 地址。
地址/范围	web 服务器的互联网 IP 地址。外部 IP 地址必须是从 web 服务器 ISP 获得的静态 IP 地址。该地址必须是不被其他主机使用唯一性的地址，该地址也不能应用虚拟 IP 的外部接口地址相同。但是，外部 IP 地址必须路由到所选的接口。虚拟 IP 地址与外部 IP 地址可以处于不同的子网。当您设置虚拟 IP 时，外部接口将对 ARP 请求作出回应。
映射到 IP/IP 地址范围	内部网络中服务器的 IP 地址范围。通过在第一个字段输入起始 IP 地址在第二个字段输入结束的 IP 地址来定义一个 IP 地址范

参数名称	参数说明
	围。
方式	设置为 TCP。设置负载平衡的方式。详细信息，参加“配置虚拟 IP”。
真实服务器	如果您对 VIP 类型设置服务器负载平衡，输入真实服务器的 IP 地址。有关真实服务器的详细信息，参见“配置虚拟 IP”。
端口转发	选中该功能框。
协议	设置为 TCP。
外部服务端口	与互联网发生通信使用的端口号。对于 web 服务器，一般通常使用的端口号为 80。

将设置了负载平衡虚拟 IP 添加到防火墙策略中。

将外部接口应用虚拟 IP 设置添加 dmz1 防火墙策略中，那么当位于互联网中的用户试图与服务器 IP 地址连接时，数据包从 wan1 接口通过 ZXSEC US 设备到达 dmz1 接口。虚拟 IP 设置将这些数据包的目的地地址从外部 IP 转换为服务器所处的 DMZ 网络的 IP 地址。

1. 进入防火墙>策略，并点击“新建”。
2. 配置防火墙策略。

参数信息

参数名称	参数说明
源接口/区域	external
源地址名称	全部（或一个具体的 IP 地址）
目标接口/区域	dmz1
目标地址名称	Load_Bal_VIP_port_forward
时间表	循环。
服务	HTTP
动作	ACCEPT（接受）

3. 点击“NAT”。
4. 点击 OK 确认。

17.4.7 添加动态虚拟 IP

动态虚拟 IP 的添加类似于虚拟 IP 的添加。区别在于外部 IP 地址必须设置为 0.0.0.0.，以便外部 IP 地址与任何 IP 都匹配。

添加动态虚拟 IP

1. 进入防火墙>虚拟 IP>虚拟 IP。
2. 点击“新建”。
3. 输入动态虚拟 IP 的名称。
4. 从列表中选择虚拟 IP 外部接口。外部接口与源网络连接接收数据包将其转发到目标网络。可以选择任何防火墙接口或 VLAN 子接口。
5. 将外部 IP 地址设置为 0.0.0.0.该地址可以与任何 IP 地址相匹配。
6. 输入外部服务端口号，配置动态端口转发。外部端口号必须与被转发数据包的目标地址端口号相匹配。例如，虚拟 IP 提供从互联网到 PPTP 服务器的 PPTP 访问，那么外部服务端口号应该设置为 1723（PPTP 端口）。
7. 设置端口转发。
8. 设置协议类型为 TCP。
9. 输入配置动态端口转发的外部服务端口号。外部服务端口号必须与数据包被转发的目标端口匹配。例如，如果虚拟 IP 提供从互联网到 PPTP 服务器的 PPTP 访问，外部服务端口号应为 1723（PPTP 端口）。
10. 输入映射端口号，该端口号添加在转发的数据包中。如果该端口没有被转换，输入与外部服务端口号相同的号码。
11. 点击 OK 确认。

添加虚拟 IP 只具有端口转换功能

添加虚拟 IP 地址时，如果您输入的虚拟 IP 地址与映射的地址相同，用于端口转发，那么目标 IP 地址将被更改，但是端口号将根据您指定的进行更改。

1. 进入防火墙>虚拟 IP>虚拟 IP。
2. 点击“新建”。
3. 输入动态虚拟 IP 的名称。
4. 从列表中选择虚拟 IP 外部接口。外部接口与源网络连接接收数据包将其转发到目标网络。可以选择任何防火墙接口或 VLAN 子接口。
5. 设置外部 IP 地址为映射 IP 地址。
6. 输入外部服务端口号，配置动态端口转发。外部端口号必须与被转发数据包的目标地址端口号相匹配。例如，内部网络中的 PPTP 服务器的 IP 地址。

7. 设置端口转发。

8. 设置协议类型为 TCP。

9. 输入配置动态端口转发的外部服务端口号。外部服务端口号必须与数据包被转发的目标端口匹配。例如，如果虚拟 IP 提供从互联网到 PPTP 服务器的 PPTP 访问，外部服务端口号应为 1723（PPTP 端口）。

10. 输入映射端口号，该端口号添加在转发的数据包中。

11. 点击 OK 确认。

17.5 虚拟 IP 地址组

您可以创建虚拟 IP 地址组，便于对防火墙策略流量的控制。例如，对于 DMZ 接口，如果您有两台邮件服务器使用虚拟 IP 映射，您可以将这两个虚拟 IP 添加组成为一个虚拟 IP 地址组（VIP 组）并创建一项外部到 DMZ 的策略，相比较于之前需要创建两项策略，此时一项策略便可以对流量进行控制。

17.6 查看虚拟 IP 组列表

进入“防火墙>虚拟 IP>VIP 组”，查看虚拟 IP 组列表。

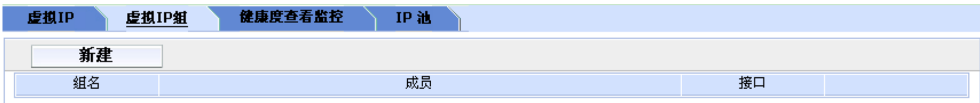


图17.6-1 VIP 组列表

VIP 组列表中的图标表示与功能如下表所示。

参数信息

参数名称	参数说明
新建	点击添加新的 VIP 组。参见“配置虚拟 IP 地址组”。
组名称	虚拟 IP 地址组的名称。
组员	组员列表。
接口	显示虚拟 IP 地址组所属的接口。
终止 IP	定义 IP 地址的结束范围。
删除图标	点击从列表中删除 VIP 组。删除图标只有在 VIP 组没有应用防火墙策略时显示。
编辑图标	点击编辑 VIP 组信息，包括组名称与成员。

17.7 配置虚拟 IP 地址组列表

进入“防火墙>虚拟 IP>VIP 组”，点击“新建”添加 VIP 组。点击对应组的“编辑”图标编辑 VIP 组。

新建虚拟IP组

组名：

接口：

loop1

可用的虚拟IP：

成员：

确定 取消

图17.7-1 编辑 VIP 组

配置以下设置并点击 OK 确认。

参数信息

参数名称	参数说明
组名称	输入或修改地址组名称。
接口	点击需要创建 VIP 组的接口。如果您正在编辑一个 VIP 组，接口的功能框显示为灰色。
可用 VIP 与成员	添加或删除成员。

17.8 IP 地址池

在 NAT 策略中启动 IP 池设置可以将数据包的源地址转换为从设置的 IP 范围中随机选择的地址，而不是局限于目标接口的 IP 地址。

IP 池（也称动态 IP 池）是添加到接口的一个 IP 地址范围，添加了 IP 池设置的接口都将对接口的 ARP 请求作出响应。

您可以在防火墙策略中启动动态 IP 池将向外的数据包源地址转换为从 IP 池中任选的地址。当策略目标接口与 IP 池接口相同时显示 IP 池列表。

在内部接口启动 IP 池设置，您可以将作为目标接口的内部接口的策略启动动态 IP

池设置。

您可以在任何接口添加多个 IP 池并在配置防火墙策略时使用 IP 池。

IP 池也可以是单个的 IP 地址。例如，192.168.110.100 同样是有效的 IP 池地址。如需要设置 IP 地址范围，您可以设置使用以下的格式：

x.x.x.x-x.x.x.x，例如 192.168.110.100－192.168.110.120

x.x.x.[x-x]，例如 192.168.110.[100－120]

IP 池与动态 NAT

您可以给动态 NAT 配置使用 IP 池。例如，您的公司或机构购买了互联网地址一个的范围，但是您的 ZXSEC US 设备外部接口只有一项到互联网连接。

您可以分配 ZXSEC US 设备的外部接口使用您公司购买的互联网 IP 地址之一。如果

ZXSEC US 设备运行于 NAT/路由模式，从您网络到互联网的连接都是通过该 IP 地址进行的。

如果您想从互联网 IP 地址发起连接，您可以将该地址范围添加到 IP 池用于外部连接。然后您可以在外部接口的策略中启动动态 IP 池作为外部接口。对于每个连接，防火墙从 IP 池中动态选择 IP 地址作为连接的源地址。其结果是，到互联网的连接显现都是从 IP 池中的任何 IP 地址发起的。

使用固定端口设置防火墙的 IP 池

如果 NAT 策略将用于连接数据包的源端口进行了地址转换，一些网络配置将不能准确的进行操作。NAT 将源端口转换以便为特殊的服务保持连接的轨迹。但是，在 NAT 策略中设置为固定端口将阻止源端口发生转换。选择固定端口意味着通过防火墙只有一项连接支持该服务。为了启动多重连接，您可以在目标接口添加 IP 池并在策略中选择动态 IP 池。防火墙将从 IP 池中任意的选择 IP 地址并将其分配给每个连接。这种情况下，防火墙支持的连接数量将取决于 IP 池中 IP 地址的数量。

源 IP 地址与 IP 池地址匹配

当源地址被转换为 IP 池的地址时，可能发生以下的情形：

- 情形 1：源地址的数量与 IP 地址池中地址相等这种情况下，ZXSEC US 设备将总会将源地址与 IP 池中的地址一一匹配。

  如果这样的情况下，您使用固定的端口，ZXSEC US 设备将保留起始的源端口。但是，如果不止一项防火墙策略使用相同的 IP 池地址，或相同的 IP 地址被应用于不止一个 IP 池中，这样便可能会导致地址冲突。

  起始地址　地址更改为

  192.168.1.1 172.16.30.1

  192.168.1.2 172.16.30.2

  ………

  192.168.1.254 172.16.30.254

- 情形 2：源地址的数量大于 IP 地址池中地址

  这种情况下，ZXSEC US 设备将使用环绕机制转换 IP 地址。

  如果这样的情况下，您使用固定的端口，ZXSEC US 设备将保留起始的源端口。但是，因为用户可能使用相同的 TCP5 进行不同的会话，这样便导致了会话冲突。

  起始地址　地址更改为

  192.168.1.1 172.16.30.10

  192.168.1.2 172.16.30.20

  ………

  192.168.1.10 172.16.30.19

  192.168.1.11 172.16.30.10

  192.168.1.12 172.16.30.11

  192.168.1.13 172.16.30.12

  ……….. ………..

- 情形 3：源地址的数量小于 IP 地址池中地址这种情况下，IP 池中的一些地址被使用，保持剩余的一些。

起始地址 地址更改为

192.168.1.1 172.16.30.10

192.168.1.2 172.16.30.11

192.168.1.3 172.16.30.12

没有更多的源地址，172.16.30.13 以及其他地址将不被使用。

17.9 查看 IP 地址池列表

如果 ZXSEC US 设备启动了虚拟域设置，需要对每个虚拟域分别设置 IP 池。从主菜单项列表中点击虚拟域，访问 IP 池。透明模式下，IP 池设置不可用。

进入防火墙>虚拟 IP>IP 池，查看 IP 池列表。

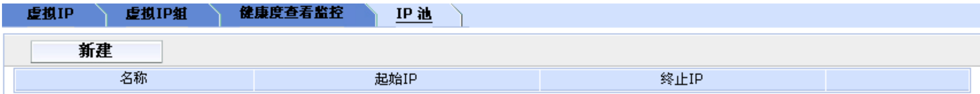


图17.9-1 IP 池列表

IP 池列表中的图标及其功能如下表所示。

参数信息

参数名称	参数说明
名称	IP 池名称。
新建	点击新建添加 IP 池。
起始 IP	定义 IP 地址的起始范围。
终止 IP	定义 IP 地址的结束范围。
删除图标	点击从列表中能够删除条目。如果 IP 池应用于防火墙策略将不能被删除。
编辑图标	点击编辑以下信息项：IP 池名称，接口，IP 范围/子网。

17.10 配置 IP 地址池

进入“防火墙>虚拟 IP>IP 池”，添加 IP 池。

新建动态IP池

名称

接口 loop1

IP地址范围/子网 0.0.0.0-0.0.0.0

确定 取消

图17.10-1 新建动态 IP 池

虚拟 IP 具有以下选项如下表所示。

参数信息

参数名称	参数说明
名称	输入 IP 池的名称。
接口	选择添加 IP 池的接口。
类型	负载平衡。
IP 范围/子网	输入 IP 池的 IP 地址范围。IP 范围是 IP 地址起始与结束的范围。起始范围必须小于结束范围。IP 地址的起始与结束范围不必与您要添加 IP 池的接口 IP 地址处于同一个子网中。

17.11 双重 NAT：IP 池与虚拟 IP 的结合

将 IP 池与虚拟 IP 结合创建防火墙策略时，您可以同时使用 IP 池与虚拟 IP 配置双重的 IP 地址和/或端口转换。举例说明，在以下的拓扑结构下：

- 在 10.1.1.0/24 子网中的用户使用端口 8080 访问服务器 172.16.1.1
- 服务器的侦听端口是 80
- 必须使用固定端口

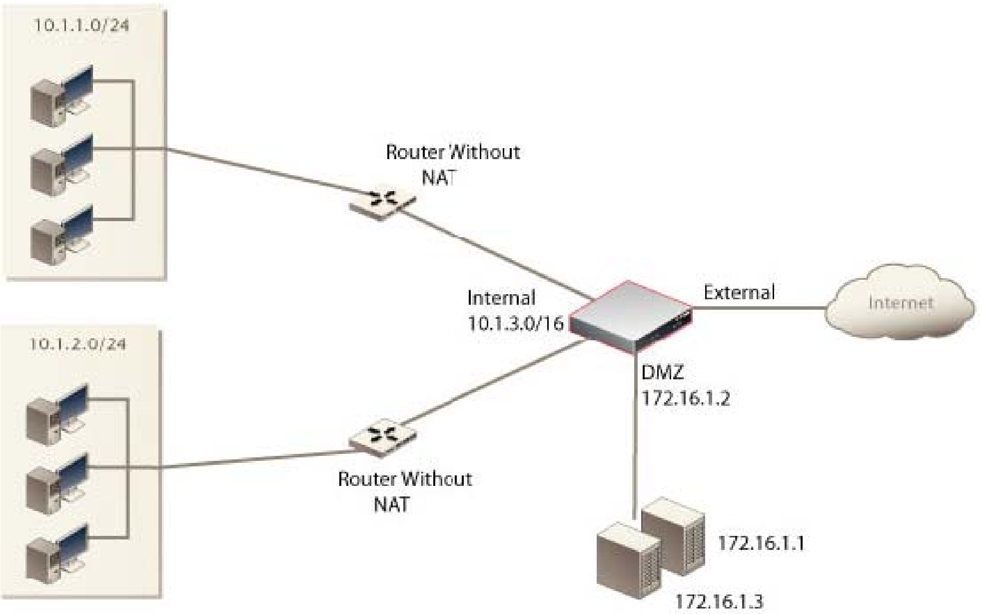


图17.11-1 双重 NAT

设置允许本地用户访问服务器，您可以使用固定的端口与 IP 池在将虚拟 IP 从 8080 转换到目标地址 80 的同时允许不止一个用户连接。

创建 IP 池

1. 进入“防火墙>虚拟 IP>IP 池”。
2. 点击“新建”。
3. 输入以下信息并点击 OK 确认。

参数信息

参数名称	参数说明
名称	Pool-1
接口	DMZ
类型	负载平衡
IP 范围/子网	10.1.3.1-10.1.3.254

创建虚拟 IP 地址只进行端口转换。

1. 进入“防火墙>虚拟 IP>虚拟 IP”。
2. 点击“新建”。
3. 输入以下信息并点击 OK 确认。

参数信息

参数名称	参数说明
名称	Server -1
外部接口	Internal
类型	静态 NAT
外部 IP 范围/子网	172.16.1.1
映射 IP 地址/范围	172.16.1.1
端口转发	启动
协议	TCP
外部服务端口	8080
映射到端口	80



注意：

该 IP 地址与服务器地址相同。

创建防火墙策略

将内部接口添加到 DMZ 防火墙策略中，配置使用虚拟 IP 转换目标端口数量以及 IP 池转换为源地址。

1. 进入“防护墙>策略”并点击“新建”。
2. 配置防火墙策略。

参数信息

参数名称	参数说明
源接口/区域	Internal
源地址名称	10.1.1.0/24
目标接口/区域	dmz
目标地址名称	Server-1
时间表	循环。
服务	HTTP
动作	ACCEPT（接受）

3. 点击 NAT。
4. 点击 OK 确认。

第18章 保护内容表

18.1 概述

描述

使用保户内容表对防火墙策略控制的流量应用不同的保护设置。本章将对在 NAT/路由以及透明模式下怎样添加保护内容表进行描述。

内容

18.2 什么是内容保护表

内容保护表是您为了满足特殊的需求而可以调整的一些设置组。保护内容表可以对防火墙控制的流量应用不同的保护设置。您可以对每项策略处理的流量类型定制不同的设置。

保护内容表可以用于：

- 对 HTTP，FTP，IMAP，POP3，SMTP 以及 IM 策略配置反病毒保护。
- 对 HTTP 策略配置 web 过滤服务。
- 对 HTTP 策略配置网页类型过滤服务。
- 对 IMAP，POP3，SMTP 策略配置反垃圾过滤服务。
- 对所有的服务启动 IPS。
- 对 HTTP，FTP，IMAP，POP3 与 SMTP 以及 IM 策略配置内容存档服务。
- 对 AIM，ICQ，MSN 以及 Yahoo 即时消息配置 IM 过滤以及访问控制。
- 对 Bit Torrent, eDonkey,Gnutella, Kazaa, Skype，以及 WinNY 点对点用户配置 P2P 访问控制与带宽控制。

- 配置日志记录哪项内容保护项。
- 对 VoIP 协议（SIP 与 SCCP）配置流速限制。

使用内容保护表，您可以对不同的防火墙策略定制不同的保护类型与级别。例如，内部与外部地址之间的流量可能需要添加比较严格的保护，被信任内部地址之间的流量可能需要中等的保护。您可以使用相同或不同的保护设置对不同的流量服务配置策略。

如果 ZXSEC US 设备启动了虚拟域设置，内部保护表可以对所有的虚拟域进行统一全局的配置。进入全局配置>防火墙>保护内容表，可以访问保护内容表。

18.3 默认的内容保护表配置

ZXSEC US 设备预先配置了四种保护内容表。多数情况下，您可以使用这些默认的保护内容设置。

参数信息

参数名称	参数说明
Strict（严格型）	适用于对 HTTP，FTP，IMAP，POP3 与 SMTP 流量应用最大限度的保护。一般情况下，不必使用 Strict（严格型）的保护设置，发现病毒攻击，需要扫描检测时，可以启用 Strict（严格型）保护。
Scan（扫描型）	针对 HTTP，FTP，IMAP，POP3，与 SMTP 内容流量采用病毒扫描与文件隔离。所有的内容服务都可以采用隔离设置。带有硬盘的 ZXSEC US 设备，如果反病毒扫描发现带有病毒的文件，将把该文件隔离到 ZXSEC US 自带的硬盘中。如果有需要，系统管理员可以恢复隔离的文件。
Web（网页内容控制型）	针对 HTTP 内容流量采取病毒扫描与网页内容屏蔽。您可以在防火墙策略中添加该保护设置来控制 HTTP 流量。
Unfiltered（无过滤型）	如果对于内容流量不愿意采用内容防护，您可以使用无过滤型保护。您可以在不需要内容保护的高可信与安全性较高的网络连接区域，在防火墙的策略中添加该保护设置。

18.4 查看内容保护表

进入“防火墙>保护内容表”，可以查看内容保护列表。

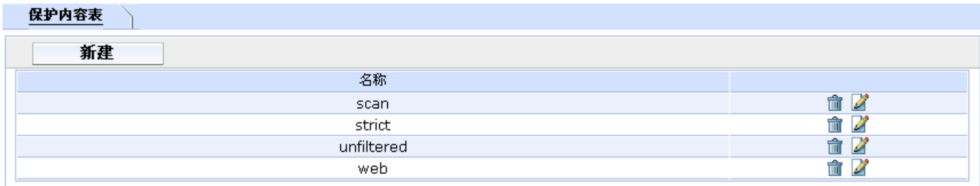


图18.4-1 默认保护内容表

保护设置中的图标以及其功能如下表所示。

参数信息

参数名称	参数说明
新建	点击新建添加保护内容表。
名称	内容保护表名称。
删除	从列表中删除保护保护内容表。如果该内容保护项被添加在防火墙策略中则不能够被删除。
编辑	修改现有的保护内容表。



注意：

如果一项保护内容被添加在防火墙策略中或是被包括在用户组中则不能删除该保护设置。

18.5 配置内容保护表

如果默认的保护内容不能够提供所需要的设置，您可以根据需要定制保护内容选项。

进入防火墙>保护内容，点击“新建”可以添加内容保护选项。

新建保护内容表

内容表名称：

注释： (最大63个字符)

- 防病毒
- Web过滤
- US Service网页过滤
- 垃圾过滤
- 入侵防护系统
- 内容存档
- IM / P2P
- VoIP
- 日志

确定 取消

图18.5-1 新建保护内容表

创建与编辑保护内容表时，您可以配置以下选项如下表所示。

参数信息

参数名称	参数说明
内容表名称	输入保护内容表的名称。
说明	如需要，输入对该内容保护项的描述。
防病毒	参见“配置反病毒选项”。
Web 过滤	参见“配置 web 过滤选项”。
Service 网页过滤	参见“配置网页类型过滤选项”。
垃圾邮件过滤	参见“配置垃圾邮件过滤选项”。
入侵防护系统	参见“配置 IPS 选项”。
内容存档	参见“配置内容存档选项”。
IM 与 P2P	参见“配置 IM 与 P2P 选项”。
VoIP	参见“配置 VoIP 选项”。
日志	参见“日志选项”。



注意：

如果同时启动了“病毒扫描”与“文件屏蔽”设置，与选项中文件模式匹配的文件在进行病毒扫描之前将先被屏蔽。

18.5.1 配置防病毒选项

防病毒

	HTTP	FTP	IMAP	POP3	SMTP	IM	NNTP	选项
防病毒扫描	☐	☐	☐	☐	☐	☐	☐	
AV数据库扩展	☐	☐	☐	☐	☐	☐	☐	
文件过滤器	☐	☐	☐	☐	☐	☐	☐	-- 无 --
允许分片的电子邮件通过			☑	☑	☑			
用户舒适	☐	☐						
时间间隔（1 - 900 秒）	10	10						
数量（1 - 10240 字节）	1	1						
文件/电子邮件超过规定大小	通过	通过	通过	通过	通过	通过	通过	
阈值（1 - 139 MB）	10	10	10	10	10	10	10	
在发出的邮件上加入签名	☐启用				(只有SMTP)			

图18.5-2　防病毒选项



注意：

NNTP 选项暂时不可用。

以下是可用的防病毒选项。

参数信息

参数名称	参数说明
防病毒扫描	对每项协议（HTTP，FTP，IMAP，POP3 与 SMTP 以及 IM）启动或禁止病毒扫描功能。如果在反病毒>配置>灰色软件中启动扫描灰色软件功能，灰色软件也在扫描之列。通过 CLI 启动启发式扫描后，该扫描也将应用于防病毒扫描项。当您设置启动病毒扫描时，限流模式也将自动启动。
文件屏蔽	对每项协议（HTTP，FTP，IMAP，POP3 与 SMTP）启动或禁止文件模式屏蔽。您可以根据文件的名称，扩展名与其它格式屏蔽文件。文件模式屏蔽对可能含有害的内容的文件的隔离具有一定的灵活性。
文件模式下拉菜单	点击选择保护内容项使用的文件模式。默认的文件模式是内嵌模式。只有 ZXSEC US1300 以及以上型号的设备支持该功能设置项。
隔离文件（需要保存日志记录的硬盘）	对每项传输协议启动或中止隔离设置。您可以查看被隔离的可疑文件或将其提交到中兴通讯公司进行分析。 如果 ZXSEC US 设备没有配置硬盘或 USLA 设备，保护内容表中不显示该选项。
允许分片的电子邮件	启动或中止通过以邮件传输协议（IMAP，POP3，SMTP）传输的分片邮件。分片邮件不能够进行病毒扫描。

参数名称	参数说明
	对 HTTP 与 FTP 流量启动或中止进程显示选项。该功能项对被缓冲的文件以及使用 HTTP 与 FTP 下载的文件提供了直观性的状态显示信息。用户可以查看网页浏览的情况或文件下载的进程。鉴于用户下载的信息数据首先存放在 ZXSEC US 设备缓存中，如果中止该选项，用户可能因为看不到缓存信息而误认为下载传输失败而取消下载任务。
时间间隔	下载任务开始之后启动进程显示之前的时间间隔。该时间也是并发流量间隔。
数量	间隔时间中的传输量。（以比特计）
超大容量文件/邮件	点击屏蔽或通过超过每项传输协议配置的阀值规定的文件与邮件。 如果文件超过设定的阀值（兆字节），根据所设定的动作可以允许通过或被屏蔽。配置扫描时最大阀值是 ZXSEC US 设备 RAM 的 10％。 **注意：** 对于邮件扫描来说，超大容量阀值是指邮件用户编码后加上附件邮件的最终大小。邮件用户可能使用各种编码类型并且一些编码类型将邮件附件转换为比原附件更大的文件。一般常用的编码方法是 base64，它将二进制数据的 3 个字节转换为 base64 数据的 4 个字节。因此，即使附件是小于配置的超大容易阀值的几个兆字节也会并屏蔽或被记录为超大容量的邮件。
在发出的邮件加上签名	创建并启动附加到向外传输邮件（只适用于以 SMTP 传输的邮件）的签名。

有关反病毒配置选项的详细信息，参见“反病毒”。

18.5.2 配置 web 过滤选项

▼ Web过滤

	HTTP	HTTPS	选项
Web内容屏蔽	☐		-- 无 -- 阈值: 10
Web内容免屏蔽	☐		-- 无 --
Web网址过滤	☐	☐	-- 无 --
ActiveX过滤	☐		
Cookie过滤	☐		
Java Applet过滤	☐		
禁止Web断点续传	☐		
阻断不合法的网址		☐	

图18.5-3　配置 web 过滤选项

以下是保护内容表中可用的 web 过滤选项。

参数信息

参数名称	参数说明
web 内容屏蔽	启动或中止基于内容屏蔽列表中禁忌词汇与模式屏蔽 HTTP 流量传输格式的网页。 web 内容屏蔽下拉列表：设置该内部保护项使用的内容屏蔽列表。只有 ZXSEC US1300 以及该型号以上的设备支持该功能。 阀值：如果一个网页中含有所要匹配的屏蔽模式的多项信息，如果这些信息结合的阀值超过所设置的阀值，那么该网页将被屏蔽。详细信息参见"查看 web 内容屏蔽列表"。
Web 内容免屏蔽	启动或中止针对 HTTP 数据流基于 URL 免除列表的 web 过滤功能。 Web 内容免屏蔽下拉列表：设置该内部保护项使用的内容免屏蔽列表。只有 ZXSEC US1300 以及该型号以上的设备支持该功能。
Web 网址过滤	启动或中止基于 URL 列表的网页过滤功能。 Web 网址下拉菜单列表：点击设置该保护内容项使用的 URL 列表。只有 ZXSEC US1300 以及该型号以上的设备支持该功能。
ActiveX 过滤	启动屏蔽 ActiveX 控制件。
Cookie 过滤	启动屏蔽 Cookie。
Java Applet 过滤	启动屏蔽 Java Applet 插件。
禁止 Web 断点续传	启动该选项，阻止已经部分下载文件继续下载。启动该选项将防止隐藏在分片文件中病毒文件的无意下载。一些文件的类型，如 PDF，分片文件可以增加下载速度，如果启动该选项可能导致下载的中断。
屏蔽无效的 URL	ZXSEC US 设备可以在 CN 上执行有效性查看，在应用 web

参数名称	参数说明
	过滤之前确认是有效的主机名称。如果 CN 不是有效的主机名称，且您启动了该选项，流量将被屏蔽。

有关 web 过滤配置选项的详细信息，参见“web 过滤”。

18.5.3 配置 US Service 网页过滤选项

US Service网页过滤

	HTTP	HTTPS
启动US Service网页过滤	☐	☐
启动跳过US Service网页过滤	☐	☐
阻断HTTP的4xx和5xx错误的内容细节	☐	
通过网址对图象进行分类(被阻断的图象将用空白替换)	☐	
当判断类别失败时允许访问该网站	☐	☐
严格阻断	☑	☑
通过域和IP地址来判断网址分类	☐	☐
屏蔽经过分类重新定向的HTTP	☐	

类别	允许	阻断	日志	允许跳过
潜在不良后果的	⊙	○	☐	☐
引起反感的或有争议的	⊙	○	☐	☐
潜在消极因素的	⊙	○	☐	☐
潜在浪费带宽	⊙	○	☐	☐
潜在不安全的	⊙	○	☐	☐
大众兴趣	⊙	○	☐	☐
商业导向	⊙	○	☐	☐
其他	⊙	○	☐	☐
不在分类中	⊙	○	☐	☐

分级	允许	阻断	日志	允许跳过
缓冲中的内容	⊙	○	☐	☐
搜索多媒体	⊙	○	☐	☐
搜索图片	⊙	○	☐	☐
搜索音频	⊙	○	☐	☐
搜索视频	⊙	○	☐	☐
垃圾邮件URL	⊙	○	☐	☐

图18.5-4 web 分类过滤选项（US Service）

以下是可用的 web 分类过滤选项。

参数信息

参数名称	参数说明
启动 Service 网页过滤（HTTP）	启动网页类别屏蔽。
启动跳过 US Service 网页过滤	启动 web 种类代替。选中该功能框，将显示替代组列表。如果没有组可用，该选项呈灰色显示。
屏蔽不在分类中的 web 站点（HTTP）	屏蔽没有经过 US Service Web 分类过滤服务进行分类的网页。

参数名称	参数说明
阻断 HTTP 4xx 与 5xx 错误内容细节(HTTP)	显示 4xx 与 5xxHTTP 错误信息的替换信息。如果 HTTP 报错被允许通过，那么恶意网站或不良网站将借助一般的错误网页避开网页类型的屏蔽。
通过网址对图象进行分类(被屏蔽的图象将被空白代替)(HTTP)	启动 US Service 基于图像 URL 对图像进行分类的功能。被屏蔽的图像 URL 将以空白网页替换。US Service 服务可以屏蔽 gif，jpeg，tiff，png 与 bmp 类型的图像。
当判断类别失败时允许访问该网站(HTTP)	当 web 过滤服务出错时允许网页通过。
严格阻断（HTTP）	严格阻断在 URL 分类正确或启动 IP 地址过滤时生效。启动 IP 地址过滤后，所有的 URL 只且具有两个种类（一种为域名，另一种为 IP 地址。)。所有的 URL 属于至少一个种类（未分类也是一个种类）且可能同时也属于一个分类类型。 启动该功能项，如果有任何的分类或种类与所分类的网站列表中被屏蔽的网站相匹配的网站将不允许被访问。中止该功能项，如果有任何的分类或种类与所分类允许访问的网站相匹配的网站将被允许访问。 举例说明，如果保护内容表屏蔽了“搜索引擎”但是允许进行图片的搜索，也就是说，URL“image.google.ca”属于搜索引擎种类与图像搜索分类。启动严格阻断后，该 URL 将被屏蔽，因为它属于搜索引擎种类。严格阻断功能撤消后，因为该 URL 属于图像引擎分类，将被允许访问。该 URL 只有在搜索引擎种类与图像搜索分类同时被屏蔽时，才不被允许访问。 该选项在默认情况下是启动的。
根据域与 IP 地址判断网址分类	启动该功能项，将选项将被请求的网站的 URL 与 IP 地址进行检查，对试图绕过 US Service 系统的其他安全隐患进行防护。但是，因为 IP 过滤不能如同 URL 过滤更新那么快，可能会导致一些误分类。 该选项在默认情况下是启动的。
类别	US Serviceweb 过滤服务提供多种网页类型进行选择过滤。您可以针对不同类型的网页采取不同的设置，如允许，屏蔽或监控，以及允许访问某个类型的网页。
分级	分类屏蔽是指屏蔽某以类别的网站。提供缓冲内容的网站，例如 Google 可以并屏蔽。提供影像、音频与视频文件搜索的网站也可以被屏蔽。所分类的网站也可以被分类到某一种类中，或不进行分类。对分类网站可以设置允许通过、屏蔽、监控或允许访问的动作。

有关网页类型屏蔽选项配置的详细信息，参见“US Service web 过滤功能”。

18.5.4 配置垃圾邮件过滤选项

垃圾过滤

	☑IMAP	☑POP3	☑SMTP	选项
US Service反垃圾邮件				
IP地址检测	☐	☐	☐	
URL检测	☐	☐	☐	
邮件奇偶校验和检测	☐	☐	☐	
提交垃圾邮件	☑	☑	☑	
IP地址黑白名单检测	☐	☐	☐	-- 无 --
反向DNS检测			☐	
E-mail地址黑白名单检测	☐	☐	☐	-- 无 --
返回邮件DNS检查	☐	☐	☐	
禁忌词汇检查	☐	☐	☐	-- 无 -- 阈值: 10
动作	标记	标记	丢弃	
标记位置	⦿主题 ○MIME报头	⦿主题 ○MIME报头	○主题 ○MIME报头	
标记格式				

图18.5-5　垃圾邮件过滤选项



注意：

NNTP 选项暂时不可用。

以下是保护内容表中可用的垃圾邮件过滤选项。

参数信息

参数名称		参数说明
US Service-反垃圾邮件	IP 地址检索	启动或中止US Service垃圾邮件过滤服务的IP地址黑名单功能。US Service 摘取 SMTP 邮件服务器的源地址并将 IP 地址发送到 US Service 服务器分析该 IP 地址是否与已知的垃圾邮件发送的 IP 地址黑名单进行匹配。如果在已知到垃圾邮件黑名单中发现该 IP 地址，US Service 将终止通讯会话。如果 US Service 没有发相匹配的 IP 地址，邮件服务器继续将该邮件发送的收件人。 有关该服务的详细信息，参见“US Service 反垃圾邮件服务”。
	URL 检索	启动或中止 US Service 垃圾邮件过滤的 URL 黑名单功能。US Service 检查邮件信息的正文并摘取正文中还有的任何 URL 链接。这些链接将被发送到 US Service 服务器在 URL 黑名单中检索是否有匹配的 URL。典型的垃圾信息包含链接到广告信息的 URL（也称为广告垃圾）。如果在 URL 中发现相匹配的 URL，US Service 终止该通讯会话。如果没有发现匹配，邮件服务器继续将该邮件发送给

参数名称		参数说明
		收件人。 有关该服务的详细信息，参见“US Service 反垃圾邮件服务”。
	邮件奇偶校验和检测	启动或中止 US Service 反垃圾邮件服务中邮件信息校验值黑名单功能。该功能将计算邮件信息的校验值并将其发送到 US Service 服务器以便识别该校验值是否列在黑名单中。ZXSEC US 设备根据服务器的响应对邮件信息采取通过、标记或屏蔽动作。
	提交垃圾邮件	启动该功能项后，所有的邮件都被标注为垃圾邮件，并将一个链接添加到信息正文。如果邮件不是垃圾邮件，只需要点击正文中的链接通知 US Service 服务中心。
IP 地址黑白名单检测		黑名单/白名单检索。启动或中止对向内的 IP 地址进行检索，查看是否与垃圾邮件过滤 IP 地址列表的地址相匹配（只适用于 SMTP 协议传输的邮件）。 IP 地址 BWL 检索下拉列表：点击设置该保护内容项使用的 BWL 列表。只有 ZXSEC US1300 以及该型号以上的设备支持该功能。
反向 DNS 检测		启动或中止在域名服务器中查找源域名（SMTP HELO 命令）。
电子邮件地址黑白名单检测		启动或中止将进入的邮件地址与配置好的垃圾过滤邮件地址列表中进行检索的功能。 电子邮件地址 BWL 检索下拉列表：点击设置该保护内容项使用的 BWL 列表。只有 ZXSEC US1300 以及该型号以上的设备支持该功能。
返回邮件的 DNS 检测		启动或中止在邮件回复指定的域名或从具有 A 或 MX 记录的地址中检索域名的功能。
禁忌词汇检索		启动或中止将邮件与配置的垃圾邮件过滤禁忌词汇列表相匹配。 禁忌词汇检索下拉列表：点击设置该保护内容项使用的禁忌词汇列表。只有 ZXSEC US1300 以及该型号以上的设备支持该功能。 阀值：如果邮件中所出现的禁忌词汇模式相结合的阀值超过了设定的阀值，该邮件信息将根据所设置的处理垃圾邮件的动作执行。详细信息参见 “查看反垃圾邮件禁忌词汇列表”。
动作		垃圾邮件过滤所采取的动作。在邮件的主题或标题中标明该邮件是垃圾邮件。对于以 SMTP 传输的邮件，如果您启动了病毒扫描或限流模式(也就是接续模式，可以从 CLI 中启动)，那么只能丢弃该垃圾邮件。(启动病毒扫描后，限流模式是自动启动的。如果不启动接续或扫描，您可以

参数名称	参数说明
	选择在邮件中标明垃圾邮件或丢弃 SMTP 垃圾邮件。您也可以设置在邮件主题中添加用户定制的词或短语，或在邮件包头中插入 MIME 包头以及数值表明该邮件是垃圾邮件。您也可以配置在事件事件中记录对垃圾邮件所采取的动作。
附加到	选择在识别为垃圾邮件的主题或 MIME 报头中附上标签。
附加内容	在识别为垃圾邮件的标签中输入标明是垃圾邮件的词语附在该邮件上。附有描述性词语的标签最多可以容纳 63 个字节的长度。



注意：

一些普通邮件的用户不能根据 MIME 报头过滤信息。在对垃圾邮件贴标签之前需要查看您的邮件用户的特性。

有关垃圾邮件过滤配置选项的详细信息，参见“垃圾邮件过滤”。

参见“配置 ZXSEC US 设备使用 US SERVICE 中心以及 US Service 服务”有关如何配置 US Service 垃圾邮件过滤服务。

18.5.5 配置 IPS 选项



图18.5-6 IPS 选项

以下是保护设置中可用的 IPS 选项。

参数信息

参数名称	参数说明
IPS 特征值	对内容保护项设置一项或多项 IPS 特征安全防护级别。可供设置的级别分别为：危急、高、中、低与消息。对应安全级别的特征如果没有被选中将不被触发。
IPS 异常	对内容保护项设置一项或多项 IPS 异常安全防护级别。可供设置的级别分别为：危急、高、中、低与消息。对应安全级别的特征如果没有被选中将不被触发。

有关 IPS 配置选项的详细信息，参见“入侵检测防护”。

18.5.6 配置内容存档选项

您可以设置在系统面板中显示 HTTP，HTTPS，FTP，IMAP，POP3 与 IM 流量的内容元信息或将全部内容存档到 USLA 设备。

您必须设置至少一项内容保护表功能，例如在对一些协议应用全部内容存档之前设置 AV 扫描、web 过滤与垃圾邮件过滤。换句话说，如果对协议不启动内容保护功能，即使您设置启动了全部内容存档的功能，这些协议也不会存档到 USLA 设备。

以 FTP 协议举例，以下列出三种内容存档的情况：

- 如果对 FTP 协议不启动 AV 扫描，但是您设置了全部内容存档，FTP 文件将不被存档到 USLA 设备，只记录元信息。
- 如果对 FTP 协议启动了 AV 扫描，但是您配置了通过大于 10MB 的文件的设置，那么大于 10MB 的文件将不被存档到 USLA 设备，只记录元信息。
- 如果对 FTP 协议设置启动 AV 扫描，但是您配置了屏蔽大于 10MB 的文件的设置，那么大于 10MB 的文件将不被存档到 USLA 设备，只记录元信息。

只有配置了 USLA 设备并启动将日志记录到 USLA 设备功能，才可以访问全部的内容存档选项。详细信息，参见“配置 USLA 设备记录日志”中的描述。

内容存档

	HTTP	HTTPS	FTP	IMAP	POP3	SMTP	NNTP
在系统面板上显示内容元信息	☑	☑	☑	☑	☑	☑	☐
日志存档至日志服务	无	无	无	无	无	无	无
将判定为垃圾邮件的邮件存档至日志服务				☐	☐	☐	☐

	AIM	ICQ	MSN	Yahoo!
在系统面板上显示内容元信息	☑	☑	☑	☑
IM日志存档至日志服务	无	无	无	无

图18.5-7 内容存档选项

以下是保护内容表中可用的内容存档选项。

参数信息

参数名称	参数说明
在系统面板中显示内容元信息	ZXSEC US 状态页面中内容概要部分显示每种类型流量的元信息。您可以查看 HTTP 流量，FTP 流量与邮件流量（IMAP，POP3 与 SMTP 的结合）的数据信息。

参数名称	参数说明
内容元信息存档至USLA	设置以下选项： 无：不存档。 摘要：将每项协议的内容元信息存档到 USLA 设备。内容元信息包括时间，日期以及目标地址信息，请求与回应大小以及扫描结果。内容存档只有在进入日志与报告>日志配置>日志设置启动 USLA 后才可以生效。 全部存档：将通过 HTTP 与 FTP 下载的文件，或通过 IMAP，POP3 与 SMTP 传输的所有邮件存档。
将垃圾邮件归档到USLA 设备	启动将垃圾邮件与正常的邮件一起进行存档。默认情况下，垃圾邮件信息不存档。
在系统面板显示元信息（AIM、ICQ、MSN 以及 Yahoo）	启动对状态页面中统计信息板块中显示的每项协议记录元信息。
在 USLA 设备上记录 IM 统计信息（AIM、ICQ、MSN 以及 Yahoo）	设置以下选项：无：不存档。 摘要：设置记录 AIM、ICQ、MSN 以及 Yahoo 这样 IM 协议的摘要信息。概要消息包括时间、日期以及源与目标地址消息内容、请求与回应的信息容量以及扫描结果。 全部存档：将全部 IM 协议传输的聊天信息存储到 USLA 设备。内容存档只有在进入日志与报告>日志配置>日志设置启动 USLA 后才可以生效。 注意： 您必须启动内容保护表中 IM 与 P2P 设置区域的 IM 选项，内容存档功能才能生效。

18.5.7 IM 与 P2P 选项

IM / P2P

	AIM	ICQ	MSN	Yahoo!	SIMPLE
阻断登陆	☐	☐	☐	☐	☐
阻断文件传输	☐	☐	☐	☐	
阻断声音	☐	☐	☐	☐	
检测非标准的端口	☐	☐	☐	☐	

	BitTorrent	eDonkey	Gnutella	KaZaa	Skype	WinNY
动作	通过	通过	通过	通过	通过	通过
限速(KBytes/s)	0	0	0	0		0

图18.5-8 IM 以及 P2P 选项

IM 以及 P2P 配置选项如下表所示。

参数信息

参数名称	参数说明
阻断登录	启动阻止用户登录 AIM，ICQ，MSN 以及 YahooIM 服务。
阻断文件传输	启动限制通过 AIM，ICQ，MSN 以及 Yahoo IM 服务进行文件传输。
阻断音频	启动限制通过 AIM，ICQ，MSN 以及 Yahoo IM 服务的语音传输。
检测非标准端口	启动检测 IM 流量传输的非标准端口。
动作	对 BitTorrent，eDonkey，Gnutella，Kazaa 以及 WinNY 点对点传输服务采取通过、阻断或限速动作。对 Skype 传输只能设置通过或阻断的动作，不可以设置限速。
限速	设置 BitTorrent，eDonkey，Gnutella，Kazaa 以及 WinNY 点对点传输速度。

在 IM 用户已经登录时所作的 IM 保护内容项设置只有在下一次用户登录时才开始生效。

有关 IM 配置选项的详细信息，参见“IM/P2P”中的描述。

VoIP 选项

ZXSEC US 设备支持对 SIP（包括 SIMPLE）与 SCCP 协议的限速。

VoIP

	SIP	SCCP
限制REGISTER请求(requests/sec/policy) (只适用于SIP)	0	
限制INVITE请求 (requests/sec/policy) (只适用于SIP)	0	
限制Call Setup(calls/min/client) (只适用于SCCP)		0

图18.5-9 VoIP 选项

参数信息

参数名称	参数说明
RIGISTER 请求限制	对 SIP RIGISTER 请求设置速率限制（每秒）。
INVITE 请求限制	对 SIP INVITE 请求设置速率限制（每秒）。
CALL 建立限制	设置通话用户端与通话管理器之间的 SCCP 通话建立的速率限制（每秒）。

18.5.8 配置日志选项

▼ 日志

	日志
防病毒	
病毒	☐
阻断的文件	☐
超过阈值的文件或邮件	☐
Web过滤	
内容阻断	☐
网址过滤	☐
ActiveX过滤	☐
Cookie过滤	☐
Java Applet过滤	☐
US Service网页过滤	
分类错误（只有HTTP）	☑
垃圾过滤	
记录垃圾邮件	☐
入侵防护系统	
记录入侵	☐
IM/P2P	
记录IM活动	☐
记录P2P活动	☐
VoIP	
记录VoIP活动日志	☐

图18.5-10　日志选项

参数信息

参数名称		参数说明
防病毒	病毒扫描	启动记录扫描发现的病毒。
	阻断的文件	启动记录所屏蔽的文件。
	超过阀值的文件或邮件	启动记录超大文件以及邮件信息。
web 过滤	内容阻断	启动对内容屏蔽进行日志记录。
	网址过滤	启动记录被屏蔽以及豁免屏蔽的 URL 的日志。
	ActiveX 过滤	启动记录被屏蔽的 Active X 插件日志信息。
	Cookie 过滤	启动记录被屏蔽的 Cookie 的日志信息。
	Java Applet 过滤	启动记录被屏蔽的 Cookie 的日志信息。
US Service 网页过滤	分类错误（HTTP）	启动记录 web 过滤错误信息。
	垃圾邮件过滤	垃圾邮件日志启动记录所检测发现的垃圾邮件信息。
入侵防护系统（IPS）	记录入侵	启动记录网络入侵的特征以及异常信息。
IM 与 P2P	记录 IM 活动	启动记录 IM 日志信息。
	记录 P2P 活动	启动记录 P2P 日志信息。
VoIP	纪录 VoIP 活动	启动纪录 VoIP 日志信息。

18.6 将内容保护表添加到防火墙策略中

您可以将保护内容配置添加到一个策略，这个策略的动作可以是允许或将服务加密设置为 ANY，HTTP，FTP，IMAP，POP3，SMTP 或包括这些服务的服务组。如果 ZXSEC US 设备中启动了虚拟域设置，内容保护设置需要添加到每个虚拟域中。访问防火墙策略，并在主菜单中点击虚拟域添加内容保护设置。

1. 进入防火墙>策略。
2. 选择您所要添加保护内容表的策略列表。例如，对内网用户从 web 下载的文件设置网络保护设置，选择一个内部到外部的策略列表。
3. 点击新建以添加一个新的策略，或选择一个策略并单击编辑。
4. 选中“保护内容表”功能框。
5. 从列表中选择保护内容选项。
6. 根据需要配置其余的策略选项。
7. 点击 OK 确认。
8. 对您要启用网络保护的任何策略重复以上步骤。

18.7 保护内容表的 CLI 配置命令



注意：

有关 CLI 命令的详细描述以及举例，ZXSEC US 设备 CLI 使用参考手册。

config firewall profile 命令

使用 config firewall profile CLI 命令可以添加，编辑或删除保护内容文件。使用保护设置对防火墙策略控制的流量应用不同的保护设置。

第19章 VPN IPSEC

19.1 概述

描述

本章是有关通过 web 管理器界面配置通道模式以及基于路由（接口模式）互联网安全协议 VPN 选项的说明。ZXSEC US 设备在通道模式下执行 IP 安全载荷封载（ESP）协议。加密数据包跟普通数据包一样能够路由到任何 IP 地址网络。互联网密钥交换（IKE）是根据预先定制的密钥或 X.509 电子证书自动执行的。您也可以在功能项中手动设置密钥。只有 NAT/路由模式可以支持接口模式。NAT/路由模式下，可以创建对 VPN 通道建立本地终端。

内容

19.2 关于 IPSec 接口模式

在您定义基于路由（接口模式）的 IPSec 通道时，同时自动创建虚拟 IPSec 接口。该接口是您在设置 IPSec 阶段 1 参数时选择的 ZXSEC US 设备本地接口。本地接口可以是一个物理接口、聚合接口、VDOM 间的连接或无线接口。

当一个 IPsec 虚拟接口能够与 VPN 对等体或用户建立阶段 1 通信连接时，该接口被认为是处于激活状态的。除非该接口与阶段 2 通道绑定，否则虚拟 IPSec 接口不能够通过通道发送数据流量。

进入系统管理>网络>接口，可以查看虚拟 IPSec 接口绑定的情况。与物理接口绑定的通道的名称将在名称栏目中显示。有关接口的详细信息，参见“接口”。



注意：

您可以设置将虚拟 IPSec 接口与一个区域绑定。

IPSec 虚拟接口与通道绑定后，均可以使用静态路由与策略路由数据流设置设定的具体的跳数路由到接口。另外，您可以创建防火墙策略使虚拟 IPSec 接口作为源或目标接口。

您可以通过以下所述的方法创建与通道模式等同的集中器：

- 在您配置集中的每对 IPSec 接口之间定义一项防火墙策略。对于拨号，相同的接口可以是源接口也可以是目标接口。如果有很多 site-to-site 的连接，这样的配置工作量就比较繁重。
- 将所有的 IPSec 接口配置到一个区域中并定义一个区域到区域的策略。详细信息以及举例说明，参见 ZXSEC US 设备 IPSecVPN 用户手册。

当 IP 流量到达本地 ZXSEC US 设备的向外接口时，该接口将作为一个 IPSec 通道的本地终端（也就是说该接口启动了 IPSec 接口模式），流量将被封装并通过物理接口转发到与 IPSec 虚拟接口绑定的区域。当远程 VPN 对等或用户发来的封装流量到达本地 ZXSEC US 设备物理接口时，ZXSEC US 将根据封装流量中的选择器来识别 IPSec 虚拟接口是否与设备物理接口发生通信。如果流量与预先定义的选择器相匹配，流量将被解封并转发到 IPSec 虚拟接口。

在流量通过 ZXSEC US 设备外向接口的过程中，ZXSEC US 设备路由流量并搜寻能够将流量转发到下一站中继路由的接口。如果 ZXSEC US 发现一条通过与具体的 VPN 通道绑定的虚拟接口这样的路由路线，流量将被封装并通过 VPN 通道被发送。在流量通过 ZXSEC US 设备向内接口的过程中，ZXSEC US 设备使用目标 IP 地址以及 ESP 数据包中的安全参数索引（SPI）识别 VPN 通道与阶段 2 的 SA（SA：Security Association）相匹配。如果发现相匹配的 SA，ESP 数据包将解密并且相关联的 IP 流量将通过 IP Sec 虚拟接口重新定向。

与具体路径相关联的防火墙策略将负责控制源与目标地址之间的所有 IP 流量。如需要，您可以配置多项防火墙策略调整进入或从基于路由的 VPN 通道发出的数据流。需要配置两项防火墙策略以支持双向的流量通过基于路由的 IPSec 通道，一项策略控制向内的流量，另一项控制向外的流量。

基于路由的 VPN 有助于简化 VPN 通道冗余。您可以对具有相同的 IP 的流量配置使用不同的跳数的路由路线。您也可以配置通过 VPN 通道交换动态（RIP，OSPF 或 BGP）路由信息。如果主要的 VPN 连接发生故障或路由的优先级别通过动态路由发生更改，将选择出一个替补路由使用冗余连接继续将流量转发。

提供故障冗余防护的简单方法便是创建一个备份 IPSec 接口。您可以使用 CLI 命令配置该选项。有关 ZXSEC US 设备的 CLI 使用参考手册，参见 moniter-phasel 关键字下的 ipsec vpn phase1-interface 命令，以及相关的配置举例。

19.3 自动密钥

在 IPSec 阶段 1 与阶段 2 互换时，可以配置两个 VPN 对等体（ZXSEC US 拨号服务器与 VPN 用户）自动生成唯一的互联网密钥交换（IKE）密钥。

进入 VPN>IPSEC>自动密钥（IKE），可以配置阶段 1 与阶段 2 中生成唯一性的密钥。

当您定义阶段 2 通道参数时，您可以选择阶段 1 参数以便对通道建立安全的连接并认证远程对等体。

自动密钥配置对通道模式与接口模式 VPN 均适用。

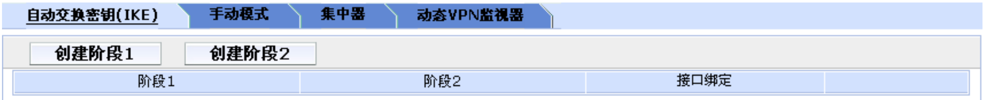


图19.3-1 自动密钥列表

参数信息

参数名称	参数说明
创建阶段 1	创建阶段 1 配置。参见“新建阶段 1”。
创建阶段 2	创建阶段 2 配置。参见“新建阶段 2”。
阶段 1	现有阶段 1 配置的名称。
阶段 2	现有阶段 2 通道配置的名称。
接口绑定	与 IPsec 通道绑定的本地接口名称。本地接口可以是物理接口、聚合接口、VDOM 间的连接或无线接口。
删除与编辑图标	删除或编辑阶段 1 配置。

19.3.1 新建 VPN 阶段 1

阶段 1 中，两个 VPN 对等体（或 ZXSEC US 拨号服务器与 VPN 用户）相互认证并交换密钥以在二者之间建立安全的通信通道。阶段 1 的基本设置建立 IPSec 阶段 1 参数与远程网关的通信协商并识别：

- 阶段 1 的各项参数进行多回合的协商确定一致的参数，该过程是在主模

式中用加码认证信息实现或是在主动模式下使用认证信息实现单个信息的一致。

- 确认远端网关是否具有匹配的预共享密钥以进行 2 个 VPN 网关或 VPN 客户端的相互认证。

- 是否是特殊标识符、证书著名名称或组名称用来在建立连接时识别远程对等体用户或客户端。

进入 VPN>IPSEC>自动密钥（IKE）并点击“新建阶段 1”，可以定义基本的 IPSec 阶段 1 参数。

新建阶段1

名称

远程网关 静态IP地址

IP 地址 0.0.0.0

本地接口 loop1

模式 野蛮模式 主模式(ID 保护)

认证方式： 预共享密钥

预共享密钥

对等体选项

接受任何对等体ID

高级选项 (XAuth, NAT 穿越, DPD)

确定 取消

图19.3-2 阶段 1 的基本设置

参数信息

参数名称	参数说明
名称	输入阶段 1 的名称。接口模式下，阶段名称的最大长度可以设定为 15 个字符；对于基于策略的 VPN 中，阶段名称长度最多可以设置为 35 个字符。如果远程网关是拨号用户，名称设置长度的最大字符数是根据建立的拨号通道数量而递减的，例如，9 个通道下为 2 个字符，99 个通道下 3 个字符，999 个通道下 3 个字符，以此类推。通道模式下的 VPN，名称应为远程连接的起始反映。对于基于路由（接口）模式下，ZXSEC US 设备也采用虚拟 IPSec 接口自动创建时的名称。
远程网关	选择远程连接的种类：

参数名称	参数说明
	● 如果具有静态 IP 地址的远程对等体将连接到 ZXSEC US 设备，设置为静态 IP 地址。 ● 如果具有动态 IP 地址的一个或多个 ZXSEC US 拨号用户或 ZXSEC US Desktop 客户端将连接到 ZXSEC US 设备，设置为连接用户。 ● 带有域名或定制了动态 DNS 服务的远程对等连接 ZXSEC US 设备时，设置为动态 DNS。
IP 地址	如果您将远程网关设置为静态 IP 地址，输入远程对等的 IP 地址。
动态 DNS	如果您将远程网关设置为动态 DNS，输入远程对等体的域名。
本地接口	该选项只有在 NAT/路由模式下可用。设置与 IPSec 通道绑定的设备物理接口、集合接口或 VLAN 接口。除非您在阶段 1 本地网关 IP 字段输入不同的 IP 地址，否则 ZXSEC US 将从系统配置>网络>接口设置中获得该 IP 地址信息。
模式	根据对等体选项设置，设置为主模式或主动模式。 ● 主模式下，阶段 1 参数与加密的认证信息进行多回合的协商。 ● 主动模式下，阶段 1 参数与不加密的认证信息进行单向的信息协商。 当远程 VPN 对等体的地址是动态分配且接受预先共享密钥验证时，您必须将模式设置为主动模式。 当远程 VPN 对等体的地址是动态分配或者远程 VPN 对等体或用户使用证书进行认证时，如果接口 IP 地址配置了多余一个的拨号阶段 1，您必须设置为主动模式。 对等选项设置可能需要特殊的模式。参见下文的对等选项配置说明。
认证方式	预共享密钥或 RSA 签名。
预共享密钥	设置为预共享密钥，输入在阶段 1 协商期间 ZXSEC US 设备用来接受远程对等或拨号客户端认证时使用的预共享密钥。您必须在远程对等体或客户端定义相同的密钥值。密钥必须是只有管理员知道的至少六位打印字符。处于网络安全考虑，密钥应该是至少 16 位的包含数字与字母混合的字符串。
认证名称	设置为 RSA 签名，输入在阶段 1 协商期间 ZXSEC US 设备用来接受远程对等或拨号客户端认证时使用的服务器证书名称。
对等体选项	● 根据远程网关与验证方式的设置，以下一项或几项选项可用。 ● 当验证方式设置为预先共享密钥，您可以选择“接受任何对等体”接受任何远程 VPN 对等体或用户的本地 ID。设置为“接受任何对等体”，ZXSEC US 不检查对等体 ID 便接受该连接。模式选项可以设置为主模式或主动模式。 ● 当验证方式设置为预先共享密钥时，可以验证具有动态 IP 地址的远程对等体或基于特殊标识符的多余一个的 ZXSEC US/US Desktop

参数名称	参数说明
	拨号用户。选择“接受”该队等 ID 并输入标识符。对于使用专用通道连接的 US DDNS 对等体或 ZXSEC US 拨号用户，该标识符数值必须与远程对等体或拨号用户阶段 1 远程网关配置中本地 ID 字段的数值相同。如果您需要对 US Desktop 用户配置验证参数，参见 US Desktop 拨号用户验证配置。如果多余一个 ZXSEC US/US Desktop 拨号用户通过相同 VPN 使用相同的标识符连接时，模式选项必须设置为主动模式。 ● 当验证方式设置为预先共享密钥时，设置为在拨号组中接受对等体 ID 来验证使用唯一的标识符与预先共享密钥(或只是唯一性的预先共享密钥)通过相同的 VPN 通道连接到 VPN 的多个 ZXSEC US/US Desktop 拨号用户。这种情况下，为了验证需要您必须创建一个拨号用户组。参见“用户组”。设置在拨号组中接 受对等体 ID，您可以从列表中选择拨号组。有关配置 ZXSEC US 拨号用户的信息，参见 ZXSEC US 设备 IPSec VPN 用户使用手册。有关配置 US Desktop 拨号用户信息，参见 US Desktop 拨号用户验证配置文件。当拨号用户使用唯一性的标识符与预先共享密钥时，模式选项必须设置为主动模式。如果拨号用户只使用预先共享密钥，而且该接口的 IP 地址中只配置了一个阶段 1 拨号用户，模式可以设置为主模式。 ● 当验证方式设置为 RSA 特征时，您可以基于特殊（或预先共享）安全证书验证一个（或多个）远程对等体或拨号用户。设置只接受该对等证书并从列表中选择对等证书的名称。对等证书在被选择之前，需要通过 CLI 命令 config user peer 添加在配置中。详细信息，参见 ZXSEC US 设备 CLI 使用参考手册中“用户”章节。如果远程 VPN 对等体或用户使用的是动态 IP 地址，将模式设置为主动模式。 ● 当验证方式设置为 RSA 特征时，您可以使用验证组验证使用动态 IP 地址的远程队等与拨号用户并使用唯一性的证书。设置只接受该对等证书并从列表中选择对等证书的名称。对等证书在被选择之前，需要通过 CLI 命令 config user peer 添加在配置中。详细信息，参见 ZXSEC US 设备 CLI 使用参考手册中“用户”章节。如果远程 VPN 对等体或用户使用的是动态 IP 地址，将模式设置为主动模式。
高级选项	定义阶段 1 参数的高级选项。参见“定义阶段 1 的高级选项”。

定义阶段 1 的高级选项

阶段 1 交互方案参数是设置 ZXSEC US 设备对于 IKE 互换用于生成密钥的加密与验证算法。高级选项中的其他设置是用来保证阶段 1 协商操作的顺利进行。

进入“VPN>IPSEC>自动密钥（IKE）”点击新建阶段 1，然后选择高级选项可以配置高级选项的操作参数。

高级选项 (XAuth, NAT 穿越, DPD)

启动IPSec接口模式

本地网关IP 主要接口IP 指定

阶段1 交互方案

1 - 加密算法 3DES 认证： SHA1

2 - 加密算法 3DES 认证： MD5

DH 组 1 2 5

密钥周期 28800 (120-172800 秒)

本地ID (可选项)

XAuth 禁用 作为客户机启用 作为服务器启用

NAT穿越 启用

保持连接的频率 10 (10-900 秒)

对等体状态探测 启用

图19.3-3 阶段 1 高级设置

参数信息

参数名称	参数说明
启动 IPSec 接口模式	对 VPN 通道的本地终端创建虚拟接口。该选项在透明模式下不可用。
本地网关 IP	如果选中“启动 IPSec 接口模式”功能框，您需要对 VPN 通道的本地终端指定一个 IP 地址。以下是可选项： ● 主接口 IP 地址；ZXSEC US 设备从系统管理>网络配置>接口设置获取 IP 地址。（参见“接口”） ● 指定；指定一个 IP 地址。对当前阶段 1 本地接口字段中选定的物理接口，集合接口或 VLAN 接口指定一个 IP 地址。 透明模式下的 VDOM 不支持接口模式配置。
阶段 1 交互方案	设置为了保护通信协商而使用的生成密钥的加密与认证算法。根据需要添加或删除加密与认证算法。最少设置一项，最多设置三项的结合。远程对等或用户端必须配置使用至少您所定义的至少一项交互方案。您可以设置使用以下任何一种对称密钥算法： ● DES，使用一个 56 个字节密钥的十六进制密文算法。 ● 3DES 硬件加密，纯文本文件使用三重密码加密三次。 ● AES128-A，使用一个 128 位字节的 128 位字节分组算法。

参数名称	参数说明
	● AES192-A，使用一个 192 位字节的 128 位字节分组算法。 ● AES256-A，使用一个 256 位字节的 128 位字节分组算法。 您可以任选以下一种信息摘要检查阶段 1 协通信协商期间信息的真实性： ● MD5，信息摘要算法。该算法是 RSA Security 公司开发的散列算法。 ● SHA1，是一种产生 160 位 Hash 值的单向 Hash 算法。点击加号键添加加密与认证的结合。
DH 组	从 DH 组选项 1，2，5 中选择一个或多个 Diffie-Hellman 组。当使用主动模式时，DH 组不能够进行协商。 ● 如果两个 VPN 对等体（或一个 VPN 服务器与其用户）均使用静态 IP 地址并在主动模式下，选择单个 DH 组。ZXSEC US 设备中的设置必须与远程对等或用户端的设置相同。 ● 当 VPN 对等体或用户端使用的是动态 IP 地址并在主动模式下，ZXSEC US 设备中最多可以选择三个 DH 组，远程对等或拨号用户端可以选择一个 DH 组。远程对等体或用户端的设置必须与 ZXSEC US 设备所选择的其中的 DH 组之一的设置相同。 ● 如果 VPN 对等体或用户端使用主模式，您可以选择多个 DH 组。远程对等或用户端至少一项设置必须与 ZXSEC US 设备所选择的 DH 组的设置相同。
密钥周期	IKE 加密密钥的有效期。密钥过期后，会生成新的密钥不间断服务。密钥的寿命可以是从 120 到 172800 秒。
本地 ID	如果 ZXSEC US 设备作为 VPN 用户端，您通过对等体 ID 进行验证，ZXSEC US 将该验证码在与阶段 1 进行通信协商的时候发送到 VPN 服务器。如果 ZXSEC US 设备作为 VPN 用户端并且您使用安全证书进行验证，本地服务器证书的著名名称可以用于认证使用。如果 ZXSEC US 设备作为拨号用户端，将不与其它拨号用户共享通道（也就是说，该通道将为该 ZXSEC US 拨号用户专用），将模式设置为主动。
XAuth	该选项支持对拨号用户的认证。如果 ZXSEC US 设备作为一个拨号用户端，选中“作为用户机启用”，输入 ZXSEC US 用来取得远程 XAuth 服务器认证的用户名与密码。如果远程网关设置为拨号用户，并且拨号用户将作为拨号组中的成员进行验证，ZXSEC US 设备可以充当作为 XAuth 服务器。选中“作为服务器启用”功能框，您必须先要创建一个用户组用于识别在 ZXSEC

参数名称	参数说明
	US 设备之后访问网络的拨号用户。您必须也配置 ZXSEC US 设备将认证请求转发到外部 RADIZXSEC US 或 LDAP 认证服务器。 参见“配置 RADIUS 服务器”以及“配置 LDAP 服务器”。 服务器类型设置确定 ZXSEC US 设备、XAuth 用户端与外部验证服务器之间使用的加密方法类型并从“用户组列表”中选择用户组。
Nat 穿越	如果本地 ZXSEC US 设备与 VPN 对等或用户端之间存在 NAT 设备时启动该选项。本地 ZXSEC US 设备与 VPN 对等体或用户端必须具有相同的 NAT 穿越设置（同时选择或取消该设置）。
保持连接的频率	如果启动 NAT 穿越，输入激活频率设置。该设置的值表示 0 到 900 秒的间隔。
对等状态探索测	启动该选项在闲置连接后重新建立 VPN 通道，根据需要可以取消该选项。该设置是用于通报通道是否通信正常；启动该选项可以保持通道在没有流量生成的时候也是呈开放状态（例如，拨号用户或动态 DNS 对等体定期更改 IP 地址时会暂时中止流量）。 启动该选项后，您可以使用 config vpn ipsec phasel（通道模式）或 config vpn ipsec phasel-interface（接口模式）CLI 命令设定闲置时间、重试次数以及重试间隔。详细信息，参见“ZXSEC US 设备 CLI 使用参考手册”。

19.3.2 新建 VPN 阶段 2

IPSec 阶段 1 通信协商完成后，开始阶段 2 通信。设置阶段 2 的参数以定义 ZXSEC US 设备用于传输剩下的通信会话使用的加密算法。阶段 2 通信过程中，具体的 IPSec SA 需要所设置的安全服务以及建立通道来执行。

阶段 2 设置是 IPSec 阶段 2 参数与阶段 1 配置的结合并对 VPN 通道的远程终端作了说明。多数情况下，您只需要配置基本的阶段 2 设置。

进入“VPN>IPSEC>自动密钥（IKE）”并点击“新建阶段 2”，配置阶段 2 设置。

新建阶段2

名称

阶段1 -----静态IP地址-----

高级选项

确定 取消

图19.3-4 新建阶段 2

参数信息

参数名称	参数说明
新建	点击新建创建新的阶段 2 通道配置。
阶段 1	点击选择分配到该通道的阶段 1 配置。参见“新建阶段 1 配置”。阶段 1 的配置是有关在该通道中远程 VPN 对等体是以何种方式被验证以及如何保证到远程对等体或用户连接的安全性。
高级选项	定义阶段 2 的高级的设置。参见 “定义阶段 2 的高级设置”。

定义阶段 2 的高级设置

阶段 2 中，ZXSEC US 设备与 VPN 对等体或用户再一次相互交换密钥以在它们之间建立安全的连接。高级阶段 2Proposal 参数将选择为了保护 SA（安全联合）而生成密钥的加密与验证算法。使用 Diffie-Hellman 自动生成密钥。

阶段 2 高级选项中其他的设置项可以加强通道通信的正常运行。进入 VPN>IPSEC>自动密钥（IKE）并点击 “新建阶段 2” 中 “高级选项” 可以配置阶段 2 的高级设置选项。

新建阶段2
名称
阶段1 -----静态IP地址-----
高级选项
阶段2 交互方案 1-加密算法: 3DES 认证算法: SHA1
2-加密算法: 3DES 认证算法: MD5
启用数据重演检测
启用完全转发安全性(PFS).
DH 組 1 2 5
密钥周期: 秒 1800 (秒) 4608000 (K字节)
保持存活 启用
快速模式选择器 源地址 0.0.0.0/0
源端口 0
目标地址 0.0.0.0/0
目标端口 0
协议 0
确定 取消

图19.3-5　阶段 2 高级设置

参数信息

参数名称	参数说明
阶段 2 阶段 2 交互方案	选择用于将数据转换为加密代码的加密与认证算法。根据需要添加或删除加密与认证算法。至少选择一项算法，最多可以选择三项算法的结合。远程对等必须配置使用所定义至少一项的交互方案。您可以设置使用以下任何一种对称密钥算法： ● NULL：不使用加密算法 ● DES：数字加密标准。是一种对称密钥算法，可以使用 40~56 位长的密钥。 ● 3DES：硬件加密，纯文本文件使用三重密码加密三次。 ● AES128-A：使用一个 128 位字节的 128 位字节分组算法。 ● AES192-A：使用一个 192 位字节的 128 位字节分组算法。 ● AES256-A：使用一个 256 位字节的 128 位字节分组算法。 您可以任选以下一种信息摘要检查阶段 1 协议通信期间信息真实性： ● Null：不使用信息摘要方法。 ● MD5：信息摘要算法。该算法是 RSA Security 公司开发的散列算法。 ● SHA1：是一种产生 160 位 Hash 值的单向 Hash 算法。 只能指定一种结合，将二次结合的加密与验证选项设置为 NULL。如果选择指定第三次加密与认证的结合，点击二次结合设置旁边的加号按键。
启动数据重演检测	启动数据重演检测。当没有经过认证的第三方截取到系列的 IPSec 数据包并将其重新放置在通道中时可能引发重放攻击。
启用完全转发安全性（PFS）	启动或禁止 PFS。当密钥过期后进行新的 Diffie-Hellman 通讯时，启用完全转发安全性（PFS）可以提高通讯的安全性。
DH 组	从 DH 组选项 1，2，5 中选择一个或多个 Diffie-Hellman 组。远程对等或用户端必须配置使用相同的组。
密钥周期	选择识别阶段 2 密钥过期的方法：秒，千字节或两者都有。如选择“两者都有”，那么超时或超过设定的 KB，密钥都会过期。时间设置可以是从 120 到 172800 秒，KB 设置的范围可以是从 5120 到 2147483648KB。
保持存活	通道不处理通讯流量时保持激活状态设置，可以启动该选项。
DHCP-IPSec	如果 ZXSEC US 设备作为一个拨号服务器并且 US DHCP 中继将对拨号用户分配 VIP 地址时，需要启动该选项。ZXSEC US 设备作为拨号用户则不能启动该选项。DHCP 中继参数必须单独配置。

参数名称	参数说明
	如果 ZXSEC US 设备作为拨号服务器并且您需要手动分配 US Desktop 拨号用户与位于拨号服务器之后的网络相匹配的 VIP 地址。启动该选项，ZXSEC US 设备可以作为拨号用户的代理服务器。 该选项只有通道模式阶段 2 配置中可用。
快速模式选择器	作为可选项，您可以设置用于 IKE 协商中作为选择器的源与目标地址。如果 ZXSEC US 设备作为拨号服务器，应该保持默认的地址，除非组成 VPN 的一个或多个私网之间发生 IP 地址混乱的问题。您可以设置为一个主机 IP 地址、一个 IP 地址范围或网络地址。您也可以设定源以及目标端口号以及协议号。 如果您需要配置现有的阶段 2 通道配置，并且通道配置在防火墙策略中用于选择器，源以及目标地址字段不可用。该选项只有通过 CLI 命令配置。参见 ZXSEC US 设备 CLI 使用参考手册中 vpn ipsec phase2 命令关键字 dst-addr-type,dst-name,src-addr-type 以及 src-name 描述信息。 ● 源地址：如果 ZXSEC US 设备作为拨号服务器，输入与位于本地 VPN 对等体之后的本地发送者或网络对应的源 IP 地址。（例如，子网中地址为 172.16.5.0 或 172.16.5.0/255.255.255.0；服务器或主机 172.16.5.1/32 或 172.16.5.1/255.255.255.255；以及一个地址范围 192.168.10.[80-100] 或 192.168.10.80-192.168.10.100）。地址为 0.0.0.0/0 表示本地 VPN 对等体之后的所有 IP 地址。如果 ZXSEC US 设备作为拨号用户，源地址必须是 ZXSEC US 拨号用户之后的私网地址。 ● 源端口：输入本地 VPN 对等体用于传输与指定服务有关的流量的端口号（协议号）。端口范围是 0 到 65535。如果设定为所有端口，输入 0。 ● 目标地址：输入与位于本地 VPN 对等体之后的本地接受者或网络对应的目标 IP 地址。（例如，子网中地址为 172.16.20.0；服务器或主机 172.16.5.1/32；以及一个地址范围 192.168.10.[80-100]）。地址为 0.0.0.0/0 表示本地 VPN 对等体之后的所有 IP 地址。 ● 目标端口：输入本地 VPN 对等体用于传输与指定服务有关的流量的端口号（协议号）。端口范围是 0 到 65535。如果设定为所有端口，输入 0。 ● 协议：输入服务的 IP 协议号。该范围可以是 1 到 255。表示所有的服务，输入 0。



注意：

您可以通过在 ZXSEC US 设备启动 VPN 用户浏览互联网。参见下文“互联网浏览配置”。

19.3.3 互联网浏览配置

您可以通过在 ZXSEC US 设备启动 VPN 用户浏览互联网。您可以通过配置防火墙策略实现该功能。有关防火墙策略的详细信息，参见“配置防火墙策略”。

基于策略的 VPN 互联网浏览配置配置一项防火墙策略，如下表所示。

参数信息

参数名称	参数说明
源接口/区域	设置 ZXSEC US 设备的公共接口。
源地址名称	设置为“全部（All)”。
目标接口/区域	设置 ZXSEC US 设备的公共接口。
目标地址名称	设置远程网络地址的名称。
动作	设置为 IPSEC。
VPN 通道	设置提供对位于 ZXSEC US 设备之后私网的访问。
内向 NAT	启动。根据需要配置其他设置。

基于策略的 VPN 互联网浏览配置

配置一项防火墙策略，如下表所示。

参数信息

参数名称	参数说明
源接口/区域	设置 IPSec 接口。
源地址名称	设置为“全部（All)”。
目标接口/区域	设置 ZXSEC US 设备的公共接口。
目标地址名称	设置为“全部（All)”。
动作	设置为 IPSEC。
NAT	启动。根据需要配置其他设置。

19.4 手工密钥

如需要，您可以手动定义建立 IPSec VPN 通道使用的密钥。

您也可以在以下情形中定义手动密钥：

- 加密和/或认证密钥的预备知识是必需的。(也就是，其中一个 VPN 对等体需要具体的 IPSec 加密和/或认证密钥)。
- 需要取消加密与认证的情况。

以上两个情形中，您不用指定 IPSec 阶段 1 与阶段 2 的参数；您可以进入 VPN>IPSEC>手动密钥选项定义手工密钥。



注意：

鉴于网络管理员必须持有密钥证书，而且在安全的环境下对远程 VPN 对等体传送更改设置很难，所以手动定义密钥可能并不安全可行。

自动交换密钥(IKE) 手动模式 集中器 动态VPN监视器

新建

VPN 通道名称	远程网关	加密算法	认证算法	

图19.4-1 IPSec VPN 手工密钥列表

参数信息

参数名称	参数说明
新建	点击新建建立新的手动密钥配置。参见 258 页“创建手动密钥配置”。
通道名称	现有手动密钥配置的名称。
远程网关	远程对等体或用户的 IP 地址。
加密算法	加密算法配置中使用的加密算法名称。
认证算法	加密算法配置中使用的认证算法名称。
删除与编辑图标	删除或编辑手动密钥配置。

创建手工密钥配置

如果其中一个 VPN 设备使用特殊的验证和加密密钥建立通道，两个 VPN 对等体必须配置相互匹配的加密与认证算法、认证与加密密钥以及互补的安全参数索引（SPI: Security Parameter Index）设置。

每个 SPI 确定一项 SA（SA: Security Association）。该数值将放置在 ESP 数据包中与 SA 链接。当接收到 ESP 数据包，收件人提交到 SPI 确定哪项 SA 应用于数据包。

每项 SA 必须手动指定一个 SPI。因为 SA 只应用于单向通讯连接，您必须指定两项 SPI（本地 SPI 与远程 SPI）适用于两个 VPN 对等之间的双向通讯连接。



警告：

如果您对安全策略、SA、选择器与 SA 数据库并不熟悉，在没有工程师协助下请慎重使用以下操作。

进入“VPN>IPSEC>手工密钥”并点击“新建”，可以为创建通道设定手动密钥。

新建手工密钥

名称	
本地SPI	100（16进制）
远程SPI	100（16进制）
远程网关	0.0.0.0
本地接口	loop1
加密算法	NULL
认证算法	NULL
IPSec接口模式	☐

确定　取消

图19.4-2　新建手工密钥

参数信息

参数名称	参数说明
名称	输入 VPN 通道名称。接口模式下，该名称最多可以为 15 个字符长度，基于策略的 VPN 中最多可以设置为 35 位字符长度。
本地 SPI	本地安全参数索引（SPI）是一个不多于八位的十六进制数（数字 0 到 9，字母 a 到 f），表示在本地 ZXSEC US 设备中处理向外的流量。有效的 SPI 的取值范围是 0xbb8 到 0xFFFFFFF。该数值必须与远程对等体中手动密钥配置的远程 SPI 值相匹配。
远程 SPI	本地安全参数索引（SPI）是一个不多于八位的十六进制数（数字 0 到 9，字母 a 到 f），表示在本地 ZXSEC US 设备中处理向内的流量。有效的 SPI 的取值范围是 0xbb8 到 0xFFFFFFF。该数值必须与远程对等体中手动密钥配置的远程 SPI 值相匹配。
远程网关	输入连接到远程对等体的公共接口的 IP 地址。该地址确定 ESP 数据包的接收人。
本地接口	该选项只有在 NAT/路由模式下可用。选择与 IPSec 通道绑定的物理接口、集合接口或 VLAN 接口的名称。ZXSEC US 设备从

参数名称	参数说明
	系统管理>网络>接口设置中获取 IP 地址。（参见“接口”）
加密算法	您可以设置使用以下任何一种对称密钥算法： ● DES：数字加密标准。是一种对称密钥算法，可以使用 40~56 位长的密钥。 ● 3DES：硬件加密，纯文本文件使用三重密码加密三次。 ● AES128-A：使用一个 128 位字节的 128 位字节分组算法。 ● AES192-A：使用一个 192 位字节的 128 位字节分组算法。 ● AES256-A 使用一个 256 位字节的 128 位字节分组算法。 加密与验证算法不能同时为 NULL。
加密密钥	选择不同的加密密钥： ● DES：输入 16 位进制字符串。（该字符串的组成可以是 0 到 9 的数字或 a 到 f 之间的字母）。 ● 3DES：输入 48 位进制的字符串。（该字符串的组成可以是 0 到 9 的数字或 a 到 f 之间的字母，以每 16 位字符进行三个分段）。 ● AES128：输入 32 位进制字符串。（该字符串的组成可以是 0 到 9 的数字或 a 到 f 之间的字母，以每 16 位字符进行二个分段）。 ● AES192：输入 48 位进制字符串。（该字符串的组成可以是 0 到 9 的数字或 a 到 f 之间的字母，以每 16 位字符进行三个分段）。 ● AES256：输入 64 位进制字符串。（该字符串的组成可以是 0 到 9 的数字或 a 到 f 之间的字母，以每 16 位字符进行四个分段）。
认证算法	● MD5，输入 48 位进制字符串。（该字符串的组成可以是 0 到 9 的数字或 a 到 f 之间的字母，以每 16 位字符进行三个分段）。 ● SHA1，输入 40 位进制字符串。（该字符串的组成可以是 0 到 9 的数字或 a 到 f 之间的字母，分别分为 16 位的片段与 24 位的片段）。 加密与验证算法不能同时为 NULL。
IPSec 接口模式	对 VPN 通道的本地终端创建虚拟接口。该命令只适用于 NAT/

参数名称	参数说明
	路由模式。

19.5 Hub&Spoke 集中器

Hub&Spoke 集中器配置中，远程对等体之间的连接可以从一个独立的中心 ZXSEC US 设备开始辐射。远程对等体之间网址与网址的连接并不存在。但是，任何两个远程对等体之间的 VPN 通道可以通过 ZXSEC US 设备充当 Hub 的作用进行建立。

在一个包含有 hub 与 spoke 的网络中，全部的 VPN 通道都以 hub 作为通道结点。与 hub 连接的对等体称为 spoke。Hub 在网络中起到集中器的作用，能够管理 spoke 之间全部的 VPN 连接。通过 hub 可以建立从一个通道到另一个通道之间的 VPN 流量连接。

进入 VPN>IPSec>集中器，定义集中器设置。

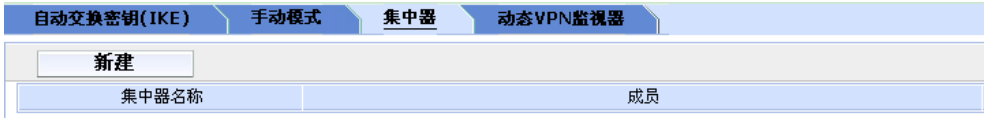


图19.5-1 IPSec VPN 集中器列表

参数信息

参数名称	参数说明
新建	点击新建在 IPSec Hub 与 Spoke 配置中定义新的集中器。参见“定义集中器选项”。
名称	现有 IPSec VPN 集中器的名称。
删除与编辑图标	删除或编辑集中器配置。
成员	与集中器连接的通道。

集中器选项

集中器配置中详细设置了 IPSec hub 与 spoke 配置中包括哪个 spoke。

进入 VPN>IPSEC>集中器中点击“新建”可以设定 IPSec hub 与 spoke 配置中 spoke。

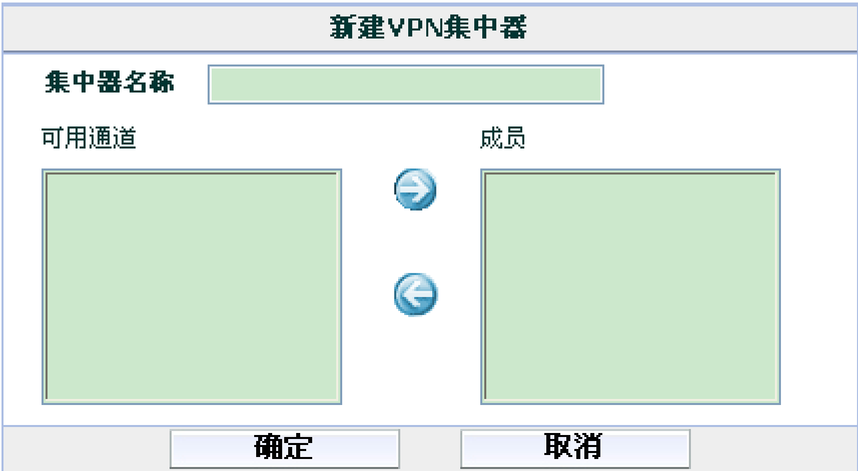


图19.5-2 在 hub 与 spoke 配置中创建新的集中器

参数信息

参数名称	参数说明
集中器名称	输入集中器的名称。
可用通道	所定义的有效 IPSec VPN 通道列表。从有效通道中使用向右的箭头选择与集中器中包含的 spoke 连接的全部通道。
成员	被选为集中器成员的通道列表。点击向左箭头，撤消与集中器连接的通道。
动态 VPN 监视器	您可以使用监控器设置查看 IPSec VPN 通道的活动状态并启动或停止这些通道。监视器设置显示包括地址列表、代理 ID 以及全部激活的通道的超时信息。

19.6 监控器

进入 VPN>IPSEC>动态 VPN 监控器，查看激活的通道。



图19.6-1 监视器列表

参数信息

参数名称	参数说明
类型	点击显示 VPN 的类型：全部，拨号，静态 IP 或动态 IP。
清除所有过滤器	点击清除应用的过滤器设置。

参数名称	参数说明
页面控制图标	显示监控 VPN 的的列表项，以及翻页功能。
名称	通道的名称。
远程网关	远程主机设备或远程主机设备之前的 NAT 设备的公共 IP 地址。
远程端口	远程主机设备或远程主机设备之前的 NAT 设备的 UDP 端口。0 表示可以使用任何端口。
代理 ID 来源	置于 ZXSEC US 设备之后的主机、服务器或私网的 IP 地址。如果在加密策略中源地址表示为一个 IP 地址范围，代理 ID 源地址栏中显示一个网络地址范围。
代理 ID 目的	网络配置的更改会影响代理 ID 目标栏中数值发生变化。 以下是网络配置发生更改是网关栏对应的变化： ● 如果不使用 VIP 地址并且远程主机直接连接到互联网，代理 ID 目标地址域显示远程主机中 NIC 的公共 IP 地址。 ● 如果不使用 VIP 地址并且 NAT 设备置于远程主机之后，代理 ID 目标地址栏显示远程主机中 NIC 的 IP 地址。 ● 如果配置使用了 VIP 地址，代理 ID 目标地址域显示属于 US Desktop 拨号用户的 VIP 地址或分配 VIP 地址的子网地址。 当 ZXSEC US 拨号用户建立通道时，代理 ID 目标地址字段显示远程私网的 IP 地址。
建立或撤消通道图标	启动或停止当前拨号通道。如果您撤消通道，拨号用户可能不得不重新建立新的 VPN 会话。

拨号通道列表提供有关已经建立的拨号用户通道状态信息。该列表包括拨号用户的 IP 地址与全部激活状态下通道的名称。列表中通道的的数量随着与拨号用户连接的状态不同而更改。

通道列表提供与具有静态 IP 地址或域名的远程对等体的 VPN 连接信息。您可以使用该列表查看每项通道配置的状态与 IP 地址信息。列表中您可以启动或撤消单个通道的通信。

第20章 VPN PPTP

20.1 概述

描述

本章是有关通过 web 管理器界面配置通道模式以及基于路由（接口模式）互联网安全协议 VPN 选项的说明。ZXSEC US 设备在通道模式下执行 IP 安全载荷封载（ESP）协议。加密数据包跟普通数据包一样能够路由到任何 IP 地址网络。互联网密钥交换（IKE）是根据预先定制的密钥或 X.509 电子证书自动执行的。您也可以在功能项中手动设置密钥。只有 NAT/路由模式可以支持接口模式。NAT/路由模式下，可以创建对 VPN 通道建立本地终端。

ZXSEC US 设备支持点对点通道协议进行两个对等体之间的 PPP 通讯流量。Windows 或 Linux PPTP 用户可以与配置作为 PPTP 服务器的 ZXSEC US 设备建立一个 PPTP 通道。您也可以配置 ZXSEC US 设置将 PPTP 数据包转送到置于 ZXSEC US 设备之后的网络中的 PPTP 服务器。

PPTP 配置只适用于 NAT/路由模式。当前 PPTP 与 L2TP 会话的最大数量为 254。起始与结束的 IP 必须在相同的 24bit 的子网中，例如 x.x.x.1-x.x.x.254。

本章是有关使用基于 web 管理器如何为 PPTP 用户设定 IP 地址范围的说明。有关如何操作其他建立 PPTP VPN 的任务，参见 ZXSEC US 设备 PPTP VPN 用户使用手册。

内容

20.2 PPTP 范围

PPTP 地址范围是指为远程 PPTP 用户保留的地址范围。当与远程 PPTP 用户连接，ZXSEC US 设备从保留的 IP 地址范围中选择分配到用户 PPTP 接口。PPTP 将分配的 IP 地址作为连接的源地址。

进入“VPN>PPTP>PPTP 范围”，可以启动 PPTP 并设置 PPTP 地址范围。设置完成后，点击“应用”生效。

编辑PPTP范围

启用PPTP

起始IP: 0.0.0.0

终止IP: 0.0.0.0

用户组:

禁用PPTP

应用

图20.2-1 PPTP 地址范围

参数信息

参数名称	参数说明
启用 PPTP	启动该选项之前您需要先添加用户组。参见“用户组”。
起始 IP	输入保留 IP 地址范围中起始 IP 地址。
终止 IP	输入保留 IP 地址范围中结束的 IP 地址。
用户组	选择您多定义的 PPTP 用户组的名称。
禁用 PPTP	选中该功能框撤消 PPTP 支持。

第21章 VPN SSL 设置

21.1 概述

描述

本章是有关通过基于 Web 的管理器配置 VPN 菜单项下 SSL 功能的描述。只有运行于 NAT/路由模式下的 ZXSEC US 设备支持 SSL VPN 功能。



注意：

有关如何配置基于 Web 模式与通道模式操作的详细说明，参见 ZXSEC US 设备 VPN SSL 设置用户手册。

内容

21.2 配置 SSLVPN

设置页面是基本的 SSL 配置，包括超时设置以及 SSL 加密优先。如需要，您也可以启动使用电子证书验证远程用户。



注意：

如需要，您可以通过使用 CLI 命令启动 SSL 版本 2 加密（与旧的浏览器相兼容）。详细信息，参见 ZXSEC US 设备 CLI 使用参考手册中“VPN”章节中有关“ssl 设置”。

进入 VPN>SSL>设置，显示当前 SSL 配置的设置。

SSL-VPN设置
启动SSL-VPN
通道IP范围 10.1.1.1 - 10.1.1.100
服务器证书 自签名
要求客户端认证
加密密钥算法 高－AES(128/256 位)与3DES
默认－RC4(128 位)与更高
低－RC4(64 位) 与更高
闲置时间阈值 300 (秒)
门户信息
高级 (DNS和WINS服务器)
DNS服务器 #1
DNS服务器 #2
WINS服务器 #1
WINS服务器 #2
应用

图21.2-1 SSL-VPN 设置

参数信息

参数名称	参数说明
启动 SSL VPN	选择复选框启动 SSL VPN 连接。
通道 IP 范围	设定为通道模式 SSL VPN 用户的 IP 地址范围。在起始与结束字段输入 IP 地址以定义 IP 地址范围。
服务器证书	点击设定用于验证使用的签订的服务器证书。如果您保持默认的设置（自签名），ZXSEC US 设备将发送出厂默认的自签证书到连接的远程用户。
要求客户端认证	如果需要使用用户组证书验证远程用户，启动该选项。然后，当远程用户发起连接时，ZXSEC US 设备切换到用户端的证书作为验证处理的一部份。

参数名称		参数说明
加密密钥算法		选择在远程 Web 浏览器客户端用户与 ZXSEC US 设备之间创建安全 SSL 连接的算法。
密钥长度	>=128bit（缺省）	如果远程用户端的 Web 浏览器能够匹配 128 位密钥或大于密码套件时，选择该选项。
	>128bit（高）	如果远程用户端的 Web 浏览器与高级的 SSL 加密相匹配，选择该选项启动密码套件，密码套件即使用多余 128 位密码加密数据。
	>=64bit（低）	如果您还不确认远程用户 Web 浏览器支持哪个级别的 SSL 加密，选择该选项启动 64 位加密或大于 64 位的密码套件。
闲置超时		在系统要求用户重新登录之前设置保持连接的时间间隔。设置范围为 10 到 28800 秒，如果不需要连接超时，您还可以设置闲置超时的值为 0。该设置应用于 SSL VPN 会话。在 Web 应用会话或通道处于活动状态时，不会出现闲置超时。
门户信息		如果您想在 Web 门户网站主页顶端显示用户信息，在该栏中键入信息。
高级（DNS 与 WINS 服务器）	DNS 服务器#1	输入提供给用户使用的最多两台 DNS 服务器。
	DNS 服务器#2	
	WINS 服务器#1	输入提供给用户使用的最多两台 WINS 服务器。
	WINS 服务器#2	

21.3 监控 SSL VPN 会话

您可以显示所有活动的 SSL VPN 会话列表信息。该列表包含远程用户的用户名称、远程用户的 IP 地址、以及连接时间信息；并确定所提供的是哪项服务。列表也显示提供的服务以及允许删除活动 Web 会话的图标。

进入 VPN>SSL>监视器，查看活动的 SSL VPN 会话列表。

设置　监视器　标签　标签组

No.	用户	源IP	开始时间	描述	动作

图21.3-1　监控列表

参数信息

参数名称	参数说明
编号（No.）	连接的编号。

参数名称	参数说明
用户	所有连接的远程用户的名称。
源 IP	与 ZXSEC US 设备连接的主机设备的 IP 地址。
开始时间	每个连接的开始时间。
描述	使用的连接服务的信息。当与一个通道模式的用户连接，该字段显示 ZXSEC US 设备分配到远程用户的 IP 地址。
删除图标	删除一个 Web 会话通道。

21.4 SSL VPN 书签

如果您创建一个用户设置只允许 Web 模式的访问，可以建立被服务器程序访问的超级链接，那么用户可以用于从主页面通过超级链接发起任何会话。使用 Web 入口应用程序，可以将 URL、IP 地址或服务器名称的应用程序添加到书签列表中。当用户发起一个活动的 SSL VPN 会话时，书签便是可用的。

21.5 查看 SSL VPN 书签列表

通过 ZXSEC US 设备，您可以显示所有现有的 SSL VPN 书签列表。列表中包括书签的名称、书签类型与链接的信息。

进入“VPN >SSL>书签”，查看预先定义的 SSLVPN 书签列表。

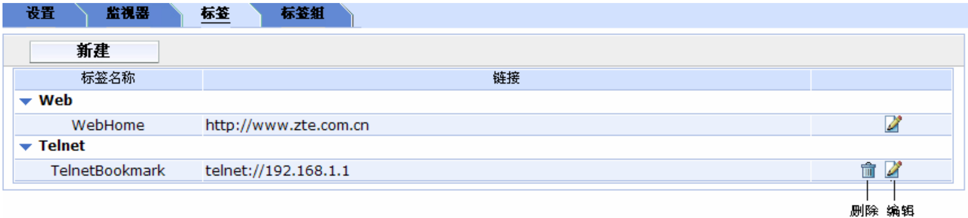


图21.5-1 书签列表

参数信息

参数名称	参数说明
书签名称	到远程服务器程序与网络服务的链接类型/名称。
链接	链接的 URL，主机名称或文件夹。
删除与编辑图标	删除或编辑列表中的条目。

21.6 配置 SSL VPN 书签

进入“VPN>SSL>书签”并点击“新建”创建服务器程序经常访问的超级链接。

新标签

标签名称

应用程序类型 Web

URL www.zte.com.cn

确定 取消

图21.6-1 新建书签

参数信息

参数名称	参数说明
书签名称	输入超级链接中显示的文本类型。书签列表中所显示的内容。
应用程序类型	在下拉菜单里选择简写的服务器程序或网络服务名称： ● Web ● Telnet ● FTP ● SMB/CIFS ● VNC ● RDP
URL/主机/文件夹	输入 ZXSEC US 设备需要将用户请求转发到正确的服务器程序或网络服务的信息类型： ● 如果应用程序类型是Web，输入Web服务器的URL（例如：www.zte.com.cn）。 ● 如果应用程序类型是 Telnet，输入 Telnet 主机的 IP 地址（例如：10.10.10.10）。 ● 如果应用程序类型是 FTP，输入 FTP 主机的 IP 地址作为根目录/文件夹（例如：//server/folder）。 ● 如果应用程序类型是 VNC，输入 VNC 主机的 IP 地址（例如：10.10.10.10）。 ● 如果应用程序类型是 RDP，输入 RDP 主机的 IP 地址（例如：10.10.10.10）。

21.7 查看 SSL VPN 书签组列表

您可以创建一个具体的书签组，将其包括在 SSL VPN 用户组的配置中。进入“VPN>SSL>书签组”，查看书签组列表。



图21.7-1 书签组列表

参数信息

参数名称	参数说明
组名称	书签组名称。
书签	用户组中可用与定义组名称的书签列表。
删除与编辑图标	删除或编辑列表中的条目。

21.8 配置 SSL VPN 书签组

进入“VPN>SSL>书签组”并点击“新建”对所选的书签创建书签组。

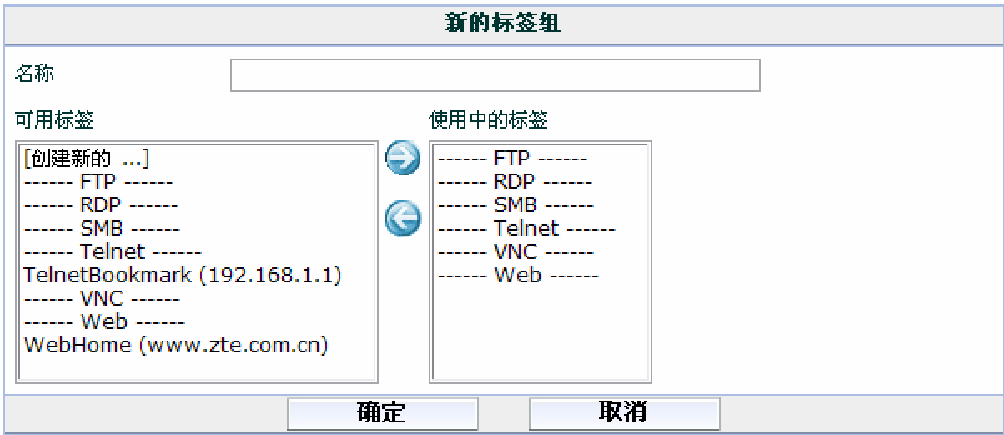


图21.8-1 新建书签组

参数信息

参数名称	参数说明
书签名称	输入超级链接中显示的文本类型。书签列表中所显示的内容。

参数名称	参数说明
可用书签	书签组中可用的书签列表。所列标签都在所属的类型下（FTP，RDP，SMB，Telnet，NVC 或 Web）。
已用书签	属于书签组的书签列表。
向右箭头按钮	书签添加到已用书签列表中。在可用书签列表中选择一个用户或服务器名称，点击将其移动到已用书签列表中。
将向左箭头按钮	将书签从已用书签列表中移除。在已用书签列表中选择一个用户或服务器名称，点击将其移动到可用书签列表中。
新建	在可用书签列表中新建书签。

第22章 VPN 证书

22.1 概述

描述

本章是有关通过基于 web 管理器如何操作并管理 X.509 安全证书的内容。就有关生成证书请求、安装已签的证书、以及导入 CA 根证书与证书撤消列表、备份与恢复已安装的证书以及私有密钥的信息进行了描述。有关证书的其他背景知识信息，参见 ZXSEC US 设备证书管理用户使用手册。

内容

22.2 本地证书

本地证书列表中显示证书请求与已安装的服务器证书条目。您提交证书请求到 CA，CA 将校验电子证书中注册的联系信息、序列号、过期时间以及 CA 的公共密钥。然后 CA 将签发证书并将证书发送返回到您，安装在 ZXSEC US 设备中。

进入“VPN>证书>本地证书”，查看证书请求以及导入已签的服务器证书。点击每个证书对应的“详细信息”图标可以查看有关证书的详细信息。列表中第一个条目对应的是 ZXSEC US 设备的自签证书，不能被删除。

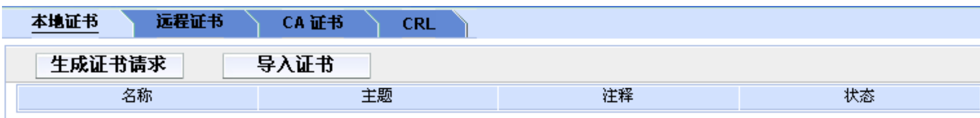


图22.2-1　本地证书列表

参数信息

参数名称	参数说明
生成证书请求	生成本地证书请求。参见“生成证书请求”。

参数名称	参数说明
导入证书	导入已签发的证书。参见“导入已签发的服务器证书”。
名称	现有证书的名称以及等待中的证书请求。
主题	本地签发证书的著名名称（DN）。
状态	本地证书的状态。 “等待中”表示证书请求需要被下载并签发。
查看证书详细信息	点击该图标，可以查看证书名称、发证方、主题以及证书有效期信息。
删除图标	删除所选的证书请求或从 ZXSEC US 设备配置中已安装的服务器证书。
下载图标	将证书请求保存到本地计算机中。发送请求到 CA 为 ZXSEC US 设备获得已签发的服务器证书。

有关证书的详细信息以及获得与安装证书的逐步操作，参见 ZXSEC US 设备证书用户手册。

证书请求的生成

ZXSEC US 设备根据您输入的用以识别设备的信息来生成证书请求。生成的请求将显示在本地证书列表中，并在状态栏中显示“等待中”。当证书请求生成后，您可以将请求下载到可以对 ZXSEC US 设备进行管理访问的计算机中，然后将请求转发到 CA。

进入 VPN>证书>本地证书，填写证书生成请求信息并点击“生成”。参见“下载并提交证书请求”有关下载以及发送证书请求的信息。

通用证书签名请求	
证书名称	
主题信息	
ID 类型	主机IP
IP	0.0.0.0
可选信息	
部门	
组织	
位置（城市）	
州/省	
国家/地区	
电子邮件	
密钥类型	RSA
密钥大小	1024 位
注册方法	⦿基于文件 ○在线SCEP
确定	取消

图22.2-2 生成证书请求

参数信息

参数名称	参数说明
证书名称	输入证书名称。一般情况下，该名称是 ZXSEC US 设备的名称。如需要可以启动将签发的证书作为 PKC12 文件导入，名称中不能包括空格。
主题信息	输入用来识别 ZXSEC US 设备的信息。 ● 主机 IP：如果 ZXSEC US 设备应用的是静态 IP 地址，选择“主机 IP”输入经过 ZXSEC US 设备公开的 IP 地址。如果 ZXSEC US 设备没有公开的 IP 地址，使用电子邮件地址（或域名）代替。 ● 域名：如果 ZXSEC US 设备使用静态 IP 地址并且设定了动态 DNS 服务，那么使用域名来识别 ZXSEC US 设备。输入 ZXSEC US 设备有效的域名。不要包括协议说明如 http:// 或任何端口号以及路径名称。如果域名不可用并且设备使用了动态 DNS 服务，那么每当 ZXSEC US 设备的公共地址更改时，用户的界面就会弹出“不能校验证书”的信息框。

参数名称	参数说明
	● 邮件地址：如果设置为使用“电子邮件”，输入 ZXSEC US 设备所有者的邮件地址。通常情况下，输入的电子邮件地址只用户用户端，而不是网关设备。
部门	所属部门名称。最多可以添加 5 个名称，+号表示添加，-表示减少。
公司	所属公司或机构的合法注册名称。
城市	ZXSEC US 设备安装的城市。
州/省	ZXSEC US 设备安装的城市所属的州或省的名称。
国家	ZXSEC US 设备安装的国家。
邮件地址	邮件地址联系信息。
密钥类型	只支持 RSA。
密钥大小	可供选择的密钥大小为 1024 比特，1536 比特或 2048 比特。更大的密钥生成证书时比较缓慢但是安全。并不是所有的 IPSecVPN 产品都支持这三种密钥。
生成方式	基于文件：设置基于文件生成证书请求。 在线 SCEP：设置在线 SCEP 通过网络自动获得已签的基于 SCEP 证书。 CA 服务器 URL：输入 SCEP 服务器的 URL，从该 URL 可以获取 CA 证书。 密码：输入 CA 服务器的密码。

下载并提交证书请求

在将证书提交到 CA 之前，您必须先填写并生成证书请求。详细信息，参见“生成证书请求”。

1. 进入 VPN>证书>本地证书。
2. 在本地证书列表中，点击生成的证书请求对应的下载图标。
3. 点击文件下载对话框中的“保存”。
4. 命名该文件并将文件另存为。
5. 将以下请求信息提交到 CA：

（1） 在管理计算机使用 web 浏览器打开 CA 网站。

（2） 根据网站中的操作说明输入 Base-64 编码的 PKCS#10 证书请求并上传证书请求。

（3） 根据 CA 中的操作说明下载 root 证书以及证书撤消列表（CRL），并将 root 证书以及 CRL 安装在每台远程用户端。

6. 从 CA 获得签发的证书后，将证书安装在 ZXSEC US 设备。参见“导入签发的服务器证书”。

导入签发的服务器证书

CA 将提供安装在 ZXSEC US 设备的已签发的服务器证书。从 CA 获得签发的证书后，将证书保存到 ZXSEC US 设备的管理计算机中。

进入 VPN>证书>本地证书并点击“导入证书”，安装签发的服务器证书。通过上传本地证书对话框安装签发的证书。证书文件可以是 PEM 或 DER 格式。其他的对话框用于导入先前输出的证书以及私有密钥。

导入证书

Type 本地证书

上传文件 浏览...

确定 取消

图22.2-3 上传本地证书

参数信息

参数名称	参数说明
上传文件	输入签发的服务器证书的名称。
浏览	浏览查找证书文件在管理计算机中存放的位置，并点击 OK 确认上传文件。

导入输出的服务器证书与私有密钥

在服务器证书与私有密钥被导入之前，先要通过 execute vpn certificate key export CLI 命令将其作为单个 PKCS12 文件输出。该文件含有一个密码，需要在导入证书文件中使用。在执行该操作之前，需要将证书文件保存到管理 ZXSEC US 设备的计算机中一份。详细信息，参见 ZXSEC US 设备证书管理用户使用手册。

进入 VPN>证书>本地证书并点击“导入证书”，导入 PKCS12 文件。

导入证书

Type PKCS12 证书

有密钥文件的证书 浏览...

密码

确定 取消

图22.2-4 上传 PKCS12 证书文件

参数信息

参数名称	参数说明
有密钥文件的证书	输入之前输出的 PKCS12 文件名称以及文件存储的路径。
浏览	在管理计算机中浏览查找 PKCS 存储的位置。
密码	输入上传 PKCS 文件所需的密码。

导入独立的服务器证书与私有密钥文件

使用上传证书对话框导入当服务器证书请求与密钥不是 ZXSEC US 设备生成的时的服务器证书以及私有密钥。这两份文件必须存储在管理计算机。

导入证书

Type 证书

上传文件 浏览...

密钥文件 浏览...

密码

确定 取消

图22.2-5 上传证书

参数信息

参数名称	参数说明
证书文件	输入证书文件存储的位置以及文件的名称。
密钥文件	输入密钥文件存储的位置以及文件的名称。
浏览	浏览查找之前输入证书文件/密钥文件的存储位置。
密码	如果需要设置密码上传并打开文件，输入密码。

22.3 远程证书

注意：

证书文件不能使用 40-bit RC2-CBC 加密。

对于撤消动态证书，将使用 OCSP（Online Certificate Status Protocol：在线证书状态协议）器。远程证书时没有私有密钥的公共证书。OCSP 只能使用 CLI 进行配置。详细信息，参见 ZXSEC US 设备 CLI 使用参考手册。



注意：

每个 vdom 只有一个 OCSP。



图22.3-1 远程证书列表

远程证书列表中，显示安装的远程（OCSP）证书。

进入“VPN>证书>远程”，查看安装的远程（OCSP）证书或导入一个远程（OCSP）证书。点击证书对应的“详细信息”图标可以查看证书的详细信息。

参数信息

参数名称	参数说明
导入证书	导入公共 OCSP 证书。参见“导入 CA 证书”。
名称	现有远程（OCSP）证书的名称。证书导入时，ZXSEC US 设备对远程（OSCP）证书分配唯一性的名称（REMOTE Cert_1,REMOTE Cert_2, REMOTE Cert_3 等）。
主题	有关远程（OCSP）证书的信息。
删除图标	从 ZXSEC US 配置中删除远程（OCSP）证书。
查看证书详细信息	查看证书的详细信息。
下载图标	将远程（OCSP）证书请求保存到本地计算机中。

导入远程（OCSP）证书

进入“VPN>证书>远程证书”，导入远程（OCSP）证书。

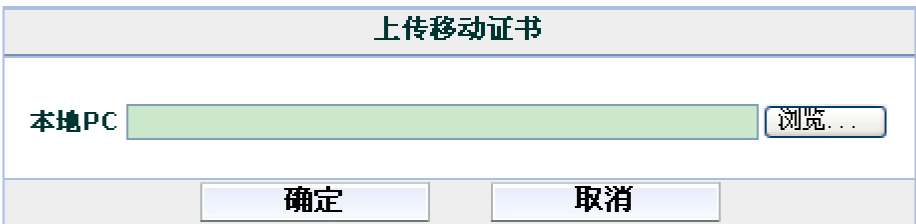


图22.3-2 上传远程证书

参数信息

参数名称	参数说明
本地 PC	使用本地管理员的 PC 上传公共证书。输入证书存储位置或点击“浏览”查看证书存储的位置。
浏览	浏览查找证书文件在管理计算机中存放的位置，并点击 OK 确认上传文件。

证书导入时，ZXSEC US 设备对远程（OSCP）证书分配唯一性的名称，名称是接续编号的（REMOTE Cert_1,REMOTE Cert_2, REMOTE Cert_3 等等）。

22.4 CA 证书

当您申请了在远程用户端安装签发的个人（管理性质）或组群证书的时候，必须从 CA 获得相应的根证书以及 CRL。

接收到签发的个人或组群证书时，根据浏览器程序文件将证书安装在远程用户。将 CA 颁发的对应的根证书与 CRL 安装在 ZXSEC US 设备。

安装后的 CA 证书将在 CA 证书列表中显示。进入 VPN>证书>CA 证书，查看安装的 CA 根证书或导入 CA 根证书。点击证书对应的“详细信息”的图标可以查看有关根证书的详细信息。

本地证书 远程证书 CA 证书 CRL
导入证书
名称 主题

图22.4-1 CA 证书列表

参数信息

参数名称	参数说明
导入证书	点击“导入证书”导入认证中心的根证书。参见“导入 CA 证书”。
名称	现有 CA 根证书的名称。CA 证书导入的时候，ZXSEC US 设备将分配给每个证书唯一的名称（如 CA_Cert_1, CA_Cert_2, CA_Cert_3 等）。
主题信息	有关认证中心的信息。
详细信息	点击该图标显示有关证书的详细信息。
删除图标	点击该图标将证书从 ZXSEC US 配置中删除。
下载图标	点击该图标可以将 CA 根证书保存到本地计算机中。

有关获得与安装电子证书的详细信息与步骤，参见 ZXSEC US 设备证书管理用户手册。

导入 CA 证书

从认证中心下载了根证书并将根证书保存在可以访问 ZXSEC US 设备的管理计算机中。进入 VPN>证书>CA 证书并点击“导入证书”，导入 CA 根证书。

上传CA证书

SCEP (SCEP服务器URL)

(可选的CA标识符)

上传文件 浏览...

确定 取消

图22.4-2 上传证书

参数信息

参数名称	参数说明
SCEP	设置使用 SCEP 服务器访问用于验证的 CA 证书。输入获取 CA 证书的 SCEP 服务器的 URL。或者，输入识别 CA 证书的信息，例如文件名。点击 OK 确认。
本地 PC	使用本地管理员的 PC 上传公共证书。输入证书存储位置或点击“浏览”查看证书存储的位置。

使用 SCEP 服务器导入证书，在点击 OK 确认后，系统将立即发起获取程序。系统对每个 CA 分配唯一性的名称。名称依次编号（如 CA_Cert_1, CA_Cert_2,CA_Cert_3 等）。

22.5 CRL

证书撤消列表（CRL）是 CA 证书签订用户与对应证书状态信息的列表。安装的 CRL 将在 CRL 列表中显示。ZXSEC US 设备使用 CRL 确保属于 CA 与远程用户的证书是有效的。

进入 VPN>证书>CRL，查看已安装的 CRL 或导入/更新 CRL。

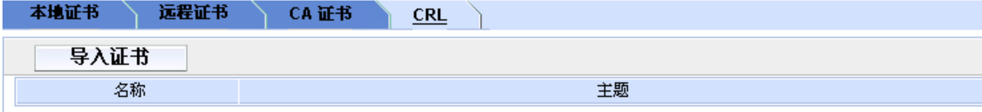


图22.5-1　证书撤消列表

参数信息

参数名称	参数说明
导入证书	导入 CRL。参见“导入证书撤销列表”。
名称	现有证书撤销列表的名称。证书撤销列表导入的时候，ZXSEC US 设备将分配给每个证书唯一的名称（如 CA_Cert_1,CA_Cert_2,CA_Cert_3 等）。
主题信息	有关证书撤销列表的信息。
删除图标	点击从 ZXSEC US 配置中删除证书撤销列表。
查看证书详细信息	显示 CRL 详细信息，如发放方与 CRL 更新日期。
下载图标	将 CRL 保存到本地计算机设备。

导入证书撤消列表

您必须定期从 CA 证人中心网站获得证书撤消列表并在 ZXSEC US 设备中更新对应的信息，以确保已经撤销证书的用户不能与 ZXSEC US 设备建立连接。从 CA 网站下载 CRL 并保存到 ZXSEC US 设备的管理计算机中。



注意：

在 LDAP，HTTP 和/或 SCEP 服务器配置了 CRL 时，当 ZXSEC US 设备中没有备份的 CRL 或当前版本过期时，将从服务器自动获取最新版本的 CRL。

进入 VPN>证书>CRL 并点击“导入”，导入证书撤销列表。

上传CRL

☐ HTTP (HTTP服务器URL)
☐ LDAP [请选择]
☐ SCEP fd
(SCEP服务器URL)
☐ 上传文件 浏览...
确定 取消

图22.5-2　上传 CRL

参数信息

参数名称	参数说明
HTTP	设置使用 HTTP 服务器获取 CRL。输入 HTTP 服务器的 URL。
LDAP	设置使用 LDAP 服务器获取 CRL。从下拉菜单中选择 LDAP 服务器。
SCEP	设置使用 SCEP 服务器获取 CRL。从下拉菜单中选择本地证书。输入获取 CRL 的 SCEP 服务器 URL。
本地 PC	使用本地管理员的 PC 上传公共证书。输入证书存储位置或点击“浏览”查看证书存储的位置。

系统对每个 CRL 分配唯一性的名称。名称依次编号（如 CRL_1,CRL_2,CRL_3 等）。

第23章 设置用户

23.1 概述

描述

本章就有关如何建立用户帐户、用户组以及外部验证服务器内容进行了说明。通过定义认证用户（或称为用户组）可以控制对网络资源的访问。

内容

23.2 配置用户验证

ZXSEC US 设备验证设置是控制用户组的访问，但是创建用户组并不是配置验证的第一步。您可以依据以下步骤配置用户验证设置：

1. 如需要外部验证，配置 RADIUS 或 LDAP 服务器。参见“RADIUS 服务器”与“LDAP 服务器”。
2. 进入用户>本地，可以配置本地用户验证。对于每个用户，您可以设置通过 ZXSEC US 设备、RADIUS 服务器或 LDAP 服务器检验密码。参见“本地用户验证”。
3. 如果您使用 Microsoft Windows 活动目录服务器进行验证，配置对该服务器的访问。参见“配置 Windows AD 服务器”。通过活动目录服务器验证的用户不需要在 ZXSEC US 设备中开设帐户。您必须在 Windows 网络安装中兴通讯服务器验证扩展（FSAE：ZTE Server Authentication Extensions）。
4. 对管理访问（HTTPSGUI），IPSec 与 SSL-VPN 使用基于证书的验证。

5. 进入“用户>用户组”创建用户组以及添加组员。用户组有三种类型，分别为防火墙、活动目录与 SSLVPN。参见“配置用户组”。对于 PKI 验证，只用防火墙与 SSLVPN 用户可以应用。

6. 进入“用户>验证>验证”可以更改验证超时或设置协议支持的选项。

23.3 本地用户验证

进入用户>本地，添加本地用户名称并配置验证。

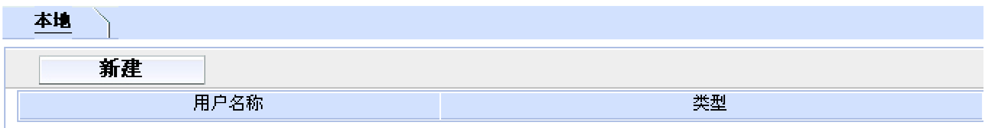


图23.3-1 本地用户列表

参数信息

参数名称	参数说明
新建	添加新的本地用户。
用户名称	本地用户名称。
类型	该用户使用的验证类型。
删除图标	删除用户。如果用户属于用户组，才不能够被删除。
编辑图标	编辑用户帐户。

注意：

删除用户的名称即删除了对该用户进行的所有配置。

配置用户帐户

进入用户>本地，并点击“新建”建立新的用户帐户。您也可以点击现有用户帐户对应的编辑图标查看或修改设置。

新建用户

用户名称

禁止

输入密码

LDAP　[请选择]

RADIUS　[请选择]

TACACS+　[请选择]

确定　取消

图23.3-2　本地用户选项

参数信息

参数名称	参数说明
用户名	输入用户名。
禁止	选中该功能框禁止该用户进行验证。
输入密码	输入用户验证使用的密码。该密码至少是 6 位字节的长度。
LDAP	选择 LDAP，通过 LDAP 服务器验证用户。选择 LDAP 服务器的名称设置用户必须认证的服务器。 注意： 您只可以选择已经添加在 USLDAP 配置中的 LDAP 服务器。参见“LDAP 服务器”。
RADIUS	选择 Radius，通过 Radius 服务器验证用户。选择 LDAP 服务器的名称设置用户必须认证的服务器。 注意： 您只可以选择已经添加在 US Radius 配置中的 Radius 服务器。

23.4 RADIUS 服务器

如果您已经配置 RADIUS 支持，并要求使用 RADIUS 服务器用户验证，ZXSEC US 设备将发送用户的信任状到 RADIUS 服务器进行验证。如果 RADIUS 服务器能够验证用户，用户也能够成功被 ZXSEC US 设备验证。如果 RADIUS 服务器不能验证用户，连接将被 ZXSEC US 设备拒绝。

注意：

默认的 RADIUS 流量端口是 1812。如果您的 RADIUS 服务器使用端口 1645，您可以使用 CLI 更改默认的 RADIUS 端口。有关 config system global 命令的详细信息，参见 ZXSEC US 设备 CLI 使用参考手册。

进入“用户>RADIUS”，配置 RADIUS 服务器。

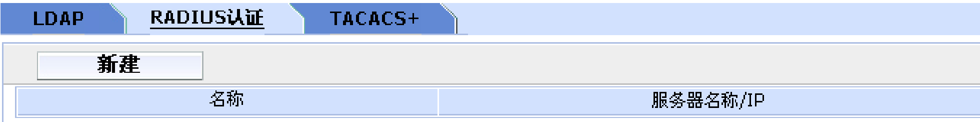


图23.4-1　RADIUS 服务器列表

参数信息

参数名称	参数说明
新建	添加新的 RADIUS 服务器。
名称	RADIUS 服务器名称。
服务器名称/IP	RADIUS 服务器的域名或 IP 地址。删除图标　删 除　RADIUS 服务器配置。 注意： 添加在用户组中的 RADIUS 服务器不可以被删除。
编辑图标	编辑 RADIUS 服务器配置。

配置 RADIUS 服务器

进入“用户>RADIUS”，并点击“新建”建立新的 RADIUS 服务器配置。您也可以点击现有服务器对应的编辑图标查看或修改设置。

新建 RADIUS 服务器

名称	
主服务器名称/IP	
主服务器秘钥	
从服务器名称/IP	
从服务器秘钥	
验证方案	◉ 用户默认验证方案 ○ 指定验证协议 MS-CHAP-v2
NAS IP/Called Station ID	
包含进所有用户组	☐ 启用

确定 取消

图23.4-2 RADIUS 配置

参数信息

参数名称	参数说明
名称	输入识别 RADIUS 服务器的名称。
一级服务器名称/IP	输入或编辑一级 RADIUS 服务器的域名以及 IP 地址。一级服务器密码 输入一级 RADIUS 服务器密码值。
二级服务器名称/IP	输入或编辑二级 RADIUS 服务器的域名以及 IP 地址。
二级服务器密码	输入二级 RADIUS 服务器密码值。
NAS IP/被呼叫机站 ID	输入或编辑 NAS IP 地址与被呼叫机站 ID（RADIUS 属性 31）。
包括在每个用户组	启动将 RADIUS 服务器自动被包括在所有用户组中。

23.5 LDAP 服务器

如果您已经配置 LDAP 支持，并要求使用 LDAP 服务器验证用户。ZXSEC US 设备将与 LDAP 服务器进行验证。使用 ZXSEC US 设置进行验证，用户需要输入用户名与密码。ZXSEC US 设置发送该用户名与密码到 LDAP 服务器。如果 LDAP 服务器通过该用户的验证，同样也成功通过 ZXSEC US 设备的验证。如果 LDAP 服务器没有通过该用户的验证，则 ZXSEC US 设备拒绝该用户发起的访问连接。

ZXSEC US 设置支持 RFC2251 定义的 LDAP 协议查找并校验用户名与密码的功能。USLDAP 支持所有的 LDAPv3.服务器。另外，ZXSEC US 的 LDAP 功能还支持基于 SSL/TLS 的 LADP 服务器验证。

US LDAP 配置并不能延展到属性功能，如一些 LDAP 服务器可以提供的密码过期通知功能。US LDAP 配置也不提供有关验证失败的原因信息。

进入用户>LDAP，配置 LDAP 服务器。

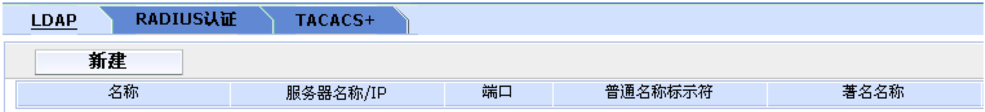


图23.5-1　LDAP 服务器列表

参数信息

参数名称	参数说明
新建	添加新的 LDAP 服务器。
名称	输入 LDAP 服务器的名称以便 ZXSEC US 设备识别。
服务器名称/IP	LDAP 服务器的域名或 IP 地址。
端口	与 LDAP 服务器发生通讯的端口。
普通名称标示符	LDAP 服务器的通用名标识符。该通用名最多可以设 20 字节的长度。大多数 LDAP 服务器的通用名标识符是 cn。但是一些服务器也使用如 uid 这样的通用名。
著名名称	著名名称在 LDAP 服务器中用于查询条目。它反映了普通名称标示符之上的 LDAP 数据库条目类的层次结构。
删除图标	删除 LDAP 服务器配置。
编辑图标	编辑 LDAP 服务器配置。

配置 LDAP 服务器

新建LDAP服务器

名称	
服务器名称/IP	
服务器端口	389
普通名称标示符	cn
著名名称	
绑定类型	简单
安全连接	

确定　取消

图23.5-2　LDAP 服务器配置

进入用户>LDAP，并点击“新建”建立新的 LDAP 服务器配置。您也可以点击现有服务器对应的编辑图标查看或修改设置。

参数信息

参数名称	参数说明
名称	输入 LDAP 服务器的名称。
服务器名称/IP	输入 LDAP 服务器的域名或 IP 地址。
服务器端口	输入与 LDAP 发生通讯的端口。默认的通讯端口是 389。 **注意：** 如果您使用安全 LDAP 服务器，默认的端口将在您设置使用的协议中显示。
普通名称标示符	输入 LDAP 服务器的通用名称标识符。大多数 LDAP 服务器的普通名标示符是 cn。但是一些服务器也使用如 uid 这样的通用名。
著名名称	输入著名名称，该名称用于在 LDAP 服务器中查询条目。使用基于 X.500 或 LDAP 格式输入服务器的著名名称。设备保持该名称并将其发送到服务器。 例如，您可以使用以下基准标识名称：ou=marketing,dc=ZTE,dc=com ou 代表机构单位，dc 是域名组成部分。您也可以指定著名名称中相同域中的多个例子。例如指定多个机构单位：ou＝accounts（会计部）ou＝marketing（市场部）dc＝ZTE dc＝com
查询图标	LDAP 服务器著名名称查询树可以用于基本著名名称的查询。 LDAP 著名名称查询列表显示 LDAP 服务器 IP 地址以及与普通

参数名称	参数说明
	名称标识符连接的所有著名的名称。树型查询有助于对 DN 字段识别恰当的条目。扩展普通名称标识符可以查看相关的 DN。从列表中选择 DN，被选 DN 将显示在著名名称字段。点击 OK 后，所选 DN 便被保存在 LDAP 服务器配置的著名名称字段中。
安全连接	设置验证使用的安全 LDAP 服务器连接。
协议	设置用于验证的安全 LDAP 协议。根据您的设置，服务器端口的值更改为所设协议的默认端口。
证书	从下拉菜单中选择用于验证的证书。进入“VPN>证书>CA 证书”查看证书列表。

23.6 PKI 验证

公共密钥架构（PKI: Public Key Infrastructure）验证是使用由对等列表、对等组和/或用户组构成的证书验证库执行验证，并返回“验证成功”或“被拒绝”这样的验证通知信息。用户只需要一个有效的证书便可以成功通过验证，而无需输入用户名或密码。

有关证书验证的详细信息，参见“ZXSEC US 设备证书管理用户手册”。配置使用 PKI 验证，只能通过 CLI 命令，详细信息参见 ZXSEC US 设备 CLI 使用参考手册。

进入“用户>PKI”配置 PKI 用户。

PKI

新建

名称	标题	CA

图23.6-1 PKI 用户列表

参数信息

参数名称	参数说明
新建	添加新的 PKI 用户。
用户名称	PKI 用户的名称。
主题	被验证用户的证书主题中出现的文本字符串。
发证方	CA 证书，用于验证用户。
删除图标	删除 PKI 用户。
编辑图标	编辑 PKI 用户。



注意：

PKI 用户列表中的以下字段对应 PKI 用户对话框中的注明的字段:

用户名称：名称。

主题：主题

CA：CA 证书。

配置 PKI 用户

进入“用户>PKI”并点击“新建”或现有 PKI 用户对应的编辑图标。

新的PKI用户

名称

标题

CA

确定 取消

图23.6-2 PKI 用户配置

参数信息

参数名称	参数说明
名称	输入 PKI 用户的名称。该字段是必添的。PKI 用户也可以使用 CLI 命令 config user peer 命令定义。详细信息，参见 ZXSEC US 设备 CLI 使用参考手册。
主题	输入被验证用户的证书主题中出现的文本字符串。该字段是可选项。
CA	输入 CA 证书，该证书将用于验证用户。该字段是可选项。



注意：

虽然“主题”与“CA”字段是可选项，但是其中之一必须进行设置。PKI 用户对话框的以下字段对应 PKI 用户列表中的注明的字段:

用户名称：名称。

主题：主题

发证方（CA 证书）：CA 证书。

23.7 Windows AD 服务器

在使用 Windows 活动目录（AD）服务器进行验证的网站中，ZXSEC US 设备可以在不需要核对用户用户名与密码的情况下验证用户。您必须配置网络安全安装中兴通讯服务器验证扩展（FSAE）并配置 ZXSEC US 设备从 Windows AD 服务器获取信息。有关 FSAE 的详细信息，参见 FSAE 技术手册。

进入用户>Windows 活动目录，配置 Windows AD 服务器。

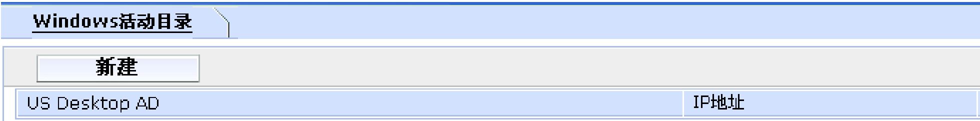


图23.7-1 Windows AD 服务器列表

参数信息

参数名称	参数说明
新建	添加新的 Windows 服务器。
名称	配置了 FSAE Windows AD 的名称。您可以扩展服务器的名称显示 Windows AD 域名组信息。
FSAE 收集器 IP	将 Windows AD 服务器登录信息发送到 ZXSEC US 设备的最多 5 个收集器代理的 TCP 端口的 IP 地址。
删除图标	删除该 Windows AD 服务器。
编辑图标	编辑该 Windows AD 服务器。
刷新图标	刷新从 Windows AD 服务器获得域名以及组信息。

配置 Windows AD 服务器

进入用户>Windows 活动目录，并点击“新建”建立新的 Windows AD 服务器配置。有关 FSAE 的详细信息，参见 FSAE 技术手册。

新建					
US Desktop AD					
ZSAE Collector IP/名称		端口	8000	密码	
ZSAE Collector IP/名称		端口	8000	密码	
ZSAE Collector IP/名称		端口	8000	密码	
ZSAE Collector IP/名称		端口	8000	密码	
ZSAE Collector IP/名称		端口	8000	密码	
LDAP 服务器					

确定　取消

图23.7-2　Windows AD 服务器配置

参数信息

参数名称	参数说明
名称	输入或编辑 Windows AD 服务器的名称。在您创建用户组时，该名称将出现在 Windows AD 服务器的列表中。
FSAE 收集器的 IP 地址	设置最多五个收集器代理的信息：输入安装了该收集器的 Windows AD 服务器的 IP 地址。
端口	输入 Windows AD 使用的 TCP 端口。该端口必须与 FSAE 收集器配置中的制定的 ZXSEC US 接听端口相同。
密码	设置收集代理的密码。只有在您配置了 FSAE 收集器代理去获得验证的访问时，该选项是需要被设置的。

23.8 配置用户组

一个用户组是用户身份的列表。该身份可以是：

- 存储在 ZXSEC US 设备中的本地用户帐户（用户名与密码）。
- 存储在 RADIUS 或 LDAP 服务器中的设置有密码的本地帐户。
- RADIUS 服务器或 LDAP 服务器（服务器中所有的身份都可以被验证）。
- Microsoft 活动目录服务器定义的用户组。

大多数情况下，ZXSEC US 是通过用户名与密码验证用户的。ZXSEC US 设备首先校验本地用户帐户。如果没有发现匹配，将继续校验用户组所属的 RADIUS 或 LDAP 服务器。发现相匹配的用户名与密码后便通过验证。

对于活动目录用户组而言，活动目录服务器在用户登录网络时对其进行验证。ZXSEC US 设备从 FSAE 收集器代理接收到用户名与密码。有关 FSAE 的详细信息，参见 FSAE 技术手册。

您可以对以下设置配置认证：

- 需要验证的防火墙策略。参见“对防火墙策略添加验证”。
- ZXSEC US 设备中的 SSL-VPN。参见“SSL-VPN 防火墙策略选项”。
- 对拨号用户配置的 IPSec VPN 阶段 1 设置。参见“创建阶段 1 配置”。
- IPSec VPN 阶段 1 的 XAuth 设置。参见“定义阶段 1 的高级设置”。
- US PPTP 配置。参见“PPTP 范围”。
- US L2TP 配置。该选项只有通过使用 config vpn l2tp CLI 命令进行配置，参见 ZXSEC US 设备 CLI 使用参考手册。
- 管理员登录时通过 RADIUS 验证。参见“配置对管理员进行 RADIUS 验证”。
- US Service Web 过滤免除组。参见“US Service-网页过滤”。

对于需要验证的每项资源，您需要设定哪些用户组被允许访问哪项资源。您可以根据验证需要来配置用户组的成员以及数量。

用户组类型

有三种类型的用户组，分别如下表所示。

参数信息

参数名称	参数说明
防火墙用户组	防火墙用户组即对需要通过验证才可以访问的防火墙类型设置的被允许访问的用户列表。该列表中列出了被允许访问的用户。当这些用户需要试图访问设置有防火墙保护的内容资源时，ZXSEC US 将通过要求这些用户的用户名与密码对其进行验证。详细信息，参见“对防火墙策略添加验证”。 防火墙用户组也可以设定对 IPSec VPN 访问的拨号用户组。在这种情况下，IPSecVPN 阶段 1 配置中拨号组对等选项中使用“接收对等 ID”设置。用户的 VPN 用户是配置了用户名作为对等 ID 以及密码作为预先共享密钥。用户只有属于该用户组并且密码与 ZXSEC US 设备中存储的密码相匹配才能够与 IPSec VPN 连接。如果用户组中的成员使用 RADIUS 或 LDAP 服务器验证则不可以成为拨号用户组。参见“创建新的阶段 1 配置”。 防火墙用户组也可以用于在 US Service 过滤功能配置中对豁免的 url 提供访问的权限。有关 US Service web 过滤的详细信息，参见“US Service-网页过滤服务”。
活动目录用户组	Microsoft Windows 网络中，ZXSEC US 设备可以允许对通过

参数名称	参数说明
	Windows 网络验证的活动目录服务器用户组成员的访问。实现该操作之前必须在网络域名控制器中安装中兴通讯服务器验证扩展（FSAE）。 活动目录用户组提供对需要活动目录验证的防火墙策略的访问成员列表。用户组的成员是指 ZXSEC US 设备从配置的 Windows AD 服务器接收到的名单中挑选的活动目录组名单。参见“Windows 活动目录服务器”。 注意： 活动目录用户组不能设置 US Service web 过滤免除或 SSLVPN 访问。
SSL-VPN 用户组 S	SL-VPN 用户组是对访问防火墙策略需要进行 SSL VPN 类型验证的用户编组。本地用户帐户、LADP 以及 RADIUS 服务器都可以是 SSL-VPN 用户组的成员。当用户访问 SSL-VPN web 门户时 ZXSEC US 需要验证用户的用户名与密码。用户组包括设置 SSL-VPN 功能的选项。参见“配置 SSL-VPN 用户组选项”。 SSL-VPN 用户组可以提供拨号用户对 IPSec VPN 的访问。在这种情况下，IPSec VPN 阶段 1 配置中拨号组队等选项中使用“接收对等 ID”设置。用户的 VPN 用户是配置了用户名作为对等 ID 以及密码作为预先共享密钥。用户只有属于该用户组并且密码与 ZXSEC US 设备中存储的密码相匹配才能够与 IPSec VPN 连接。 注意： 如果用户组中的成员使用 RADIUS 或 LDAP 服务器验证则不可以成为拨号用户组。参见“创建新的阶段 1 配置”。

用户组列表

进入用户>用户组，配置用户组。

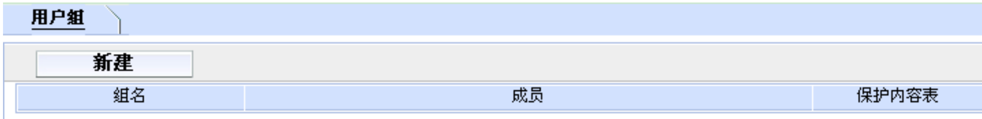


图23.8-1 用户组列表

参数信息

参数名称	参数说明
新建	添加新的用户组。
组名	用户组的名称。用户组的名称是根据不同类型的用户组列表显示的。
成员	用户组中的用户、RADIUS 服务器或 LDAP 服务器。
保护内容表	有关该用户组的保护内容设置。
删除图标	删除用户组。 注意： 包含在防火墙策略、拔号用户阶段 1 配置或 PPTP 或 L2TP 配置的用户组不能够被删除。
编辑图标	编辑用户组。

配置用户组

进入用户>用户组，点击“新建”或点击现有用户组对应的编辑图标配置用户成员以及其他选项。

新建用户组	
名称	
类别	防火墙
保护内容表	unfiltered
可用的成员 - 本地用户 - - RADIUS/LDAP/TACACS+ 服务器用户 - - PKI用户 -	组员 - 本地用户 - - RADIUS/LDAP/TACACS+ 服务器用户 - - PKI用户 -
跳过US Service Web过滤	
确定	取消

图23.8-2　用户组选项

参数信息

参数名称	参数说明
名称	输入用户组的名称。
类别	选择用户组的类型。参见“用户组类型”。
防火墙	对需要验证的防火墙策略，您可以选择该类型。参见“对防火墙策略添加验证”。
活动目录	防火墙策略中需要活动目录验证的，选择该类型的。参见“对防火墙策略添加验证”。
SSL-VPN	防火墙策略中需要 SSL-VPN 验证的，选择该类型的。参见“对防火墙策略添加验证”。
保护内容表	只有类型设置为“防火墙”或“活动目录”时，该选项才可用。您可以对该用户组设置防火墙保护内容。您也可以点击“新建”创建新的内容保护文件。
可用的成员	可以被添加到用户组的用户、RADIUS 服务器或 LDAP 服务器列表。
组员	属于用户组的用户、RADIUS 服务器或 LDAP 服务器列表。
向右箭头	点击该箭头将选中的用户或服务器添加到成员列表中。从可用用户列表中选择用户或服务器名称，点击向右箭头将其移动到成员列表中。
向左箭头	从成员列表中删除用户或服务器。从成员列表中选择用户或服务器名称，点击向左箭头将其移动到可用用户列表中。
跳过 US ServiceWeb 过滤	只有类型设置为“防火墙”时，该选项才可用。对改组配置 web 过滤免除功能。
SSL-VPN 用户组选项	只有类型设置为“SSL-VPN”时，该选项才可用。有关配置

参数名称	参数说明
	web 模式或通道模式操作的详细信息，参见 ZXSEC US 设备 SSL VPN 用户使用手册。



注意：

如果您将 LDAP 服务器或本地用户添加到用户组用于管理员验证，将发出“没有发现条目”信息。

对用户组配置跳过 US Service 过滤选项

进入用户>用户组，点击防火墙用户组的编辑图标，将该功能项扩展为跳过 US Service web 过滤列表。

跳过US Service Web过滤
允许创建US Service web过滤跳过
跳过者的范围 用户 跳过者的类型 目录
离线的URL 允许
跳过的时间 持续 询问
0 (天) 0 (小时) 15 (分钟)
可用保护配置 许可给
scan
strict
unfiltered
web

图23.8-3 跳过 US Service web 过滤配置

参数信息

参数名称	参数说明
允许跳过 USService Web 过滤	该组中的成员可以要求对 US Service web 过滤屏蔽的网页进行访问。内容保护文件将制定一个用户组作为免除组。该组中的成员可以通过 US Service web 过滤的验证访问这些被屏蔽的网页。详细信息，参见“US Service web 过滤服务”。
跳过者范围	该选项适用于需要访问被屏蔽网页用户。 用户：用户。 用户组：用户所属的用户组。

参数名称	参数说明
	IP 地址：用户 IP 地址的任何用户。 子网：用户子网中的任何用户。 验证：验证用户选择免除范围。
跳过者的类型	选择允许访问的类型。 目录：只对 URL 中最低级别的目录文件。 域名：网站的域名。 类型：US Service 类型文件。 验证：验证用户选择免除类型。
离线的 URL	选择设置用户是否能够在脱机状态下访问被屏蔽的网站。 允许：用户可以链接到其他网站。 拒绝：用户根据免除类型定义的链接只能链接到目的网站。 验证：验证用户选择是否允许使用脱机链接。
跳过的时间	设置免除的时间。 持续：设置免除的时间。 询问：验证用户识别免除时间。您所设定的的间隔是最大时间。
可用的保护内容表	可配置的内容保护表。（只适用于防火墙或活动目录用户组）。 一个内容保护表可以应用于几个用户组，且设置跳过允许。输入用户名与密码后校验用户组。尽管用户设置了跳过设置，跳过设置仍然在保护内容表中显示启动或撤消的状态。
设置允许跳过	在有的用户组中设置保护内容表使其拥有跳过权限。

配置 SSL-VPN 用户组选项

进入用户>用户组，点击编辑图标对 SSL-VPN 用户组进行编辑。将 SSL-VPN 用户组选项扩展。有关如何配置基于 web 模式或通道模式的操作，参见 ZXSEC US 设备 SSLVPN 用户手册。

SSL-VPN用户組选项

启动SSL-VPN通道服务

允许通道分割

对该組限制通道的IP地址范围 -

启动Web应用

HTTP/HTTPS代理 Telnet(applet) VNC

FTP Samba RDP

主机检测

检查US Desktop防病毒是否安装和运行

检查US Desktop防火墙是否安装和运行

检查是否安装第三方的杀毒软件

检查是否安装第三方的防火墙软件

启动清理缓存

SSL 标签

重定向URL

定制该組的入口信息

图23.8-4 SSL-VPN 用户组选项

参数信息

参数名称	参数说明
启动 SSL-VPN 通道服务	启动允许该组中的用户连接到 ZXSEC US 设备之后使用 SSL-VPN 通道的网络。该功能在透明模式下不可用。
允许分割通道	对该组设置允许通道分割。通道分割保证了只对私网的流量被发送到 SSL VPN 网关。互联网流量将通过常规的非加密路由传送。
对组限制通道 IP 范围	对组设置起始与结束 IP 地址，如果设置忽略通道 IP 范围，进入“VPN>SSL>配置”。
启动 web 应用	启动 web 门户提供到 web 应用程序的访问。透明模式下，该功能项不可用。
HTTP/HTTPS 代理，Telnet，FTP，SMB/CIFS，VNC，RDP	如果您启动了 web 应用程序，启动该组中的用户都被允许访问该应用程序。
查看是否安装并运行 US Desktop AV	只允许安装运行了 US Desktop 主机安全反病毒软件的用户连接。有关该软件的详细信息，参见中兴通讯技术手册及文件网站。
查看是否安装并运行 US Desktop FW	只允许已安装反病毒软件且软件已启动运行的用户连接。有关该软件的详细信息，参见中兴通讯技术手册及文件网站。
检查是否安装第三方的	只允许安装运行了 US Desktop 主机安全 FW 软件的用户连

<table>
<tr><th>参数名称</th><th>参数说明</th></tr>
<tr><td>杀毒软件</td><td>接。对于 Windows XP SP2 的用户所支持的产品，参见“AV/防火墙支持的产品检测”。对于其他操作系统的使用，支持使用诺顿（Symantec）反病毒或 McAfree 病毒扫描软件。

注意：
该功能项与上一个功能项不能同时设置使用。</td></tr>
<tr><td>检查是否安装第三方的防火墙软件</td><td>只允许已安装防火墙软件且软件已启动运行的用户连接。
对于 Windows XP SP2 的用户所支持的产品，参见“AV/防火墙支持的产品检测”。对于其他操作系统的使用，支持使用诺顿（Symantec）反病毒或 McAfree 病毒扫描软件。

注意：
该功能项与上一个功能项不能同时设置使用。</td></tr>
<tr><td>启动清理缓存</td><td>清除用户设备登录与退出造成的暂时性文件。该任务由 IE 浏览器下载的 ActiveX 控件，或 Firefox 下的插件执行。该设置适用于 Windows2000/windows XP 系统下 IE 与 Firefox。

注意：
如果用户的浏览器不能安装并运行缓存清除程序，该用户将不会允许访问 SSLVPN 入口。</td></tr>
<tr><td>书签</td><td>启动允许 SSLVPN 用户组使用预先定义的书签组。</td></tr>
<tr><td>重定向 URL</td><td>作为备选项，您可以在打开 SSL VPN web 门户时对该 URL 打开第二个浏览器窗口。该 URL 的 web 服务器必须存在于 ZXSEC US 设备后的私网。您也可以修改 SSL-VPNweb 门户登录页面。详细信息，参见“更改 SSL-VPN 登录信息”。</td></tr>
<tr><td>定制该组的用户信息</td><td>如果您想显示该用户组的用户 web 门户主页标题，输入信息。</td></tr>
<tr><td>限制通道的 IP 地址范围</td><td>对该用户组设定一个 IP 地址范围优先于 VPN>SSL>设置中定义的通道 IP 范围。</td></tr>
</table>

V/防火墙产品支持的检测范围

产品	AV	防火墙
Norton Internet Security 2006	Y	Y
Trend Micro PC-cillin	Y	Y
McAfee	Y	Y
Sophos Anti-virus	Y	N
N Panda Platinum 2006 Internet Security	Y	Y
F-Secure	Y	Y
Secure Resolutions	Y	Y
Cat Computer Servies	Y	Y
AhnLab	Y	Y
Kaspersky	Y	Y
ZoneAlarm	Y	Y

23.9 配置对等体与对等组

您可以在 VPN 配置中定义用于验证的对等体与对等组。使用 CLI 命令 config user peer 与 config user peergrp 配置该选项。详细信息，参见 ZXSEC US 设备 CLI 使用参考手册中“用户”章节。

验证设置

您可以对用户验证设置全局设置，包括验证超时，与验证证书。验证超时设置是控制在用户在做重新登录之前保持上次通过的防火墙验证的时间。

防火墙策略中启动用户验证时，验证通常对以下四种协议的任何一种发出（根据连接协议而定）：

- HTTP（可以被重新定向到 HTTPS）
- HTTPS
- FTP
- Telnet

该配置可以在验证配置中的协议支持列表中进行设置。用户必须首先与所支持的协议连接，才可以陆续连接到其他协议。如果 HTTPS 被设置为协议支持的选项，用户将被允许使用定制的本地证书进行验证。

当您在防火墙策略中启动用户验证时，适用防火墙策略的终端用户都将被要求通过验证。在要求输入用户名与密码的验证中，用户按要求输入用户名与密码。对于证书验证（HTTPS 或 HTTP 被重新定向到 HTTPS），您可以在 ZXSEC US 设备

上安装定制的证书，同时，终端用户也需要在其计算机设备的浏览器中安装定制的证书。否则，终端用户界面将出现警告信息且必须接受默认的 ZXSEC US 设备，而这样的证书对于终端用户的浏览器来说可能被认为是非法的。



注意：

在您使用证书验证时，如果您在创建防火墙策略时没有制定任何证书，默认将应用全局设置。如果您指定了使用的证书，基于每项策略的设置将覆盖全局设置。有关如何使用证书验证的信息，参见 ZXSEC US 设备证书管理用户手册。

进入“用户>验证>验证”，培植用户验证全局设置。

配置验证

验证超时 5 (1-480 分)

支持协议 HTTP 重定位HTTP质询到HTTP安全通道

HTTPS

FTP

Telnet

证书

应用

图23.9-1 验证设置

23.10 验证设置

参数信息

参数名称	参数说明
验证超时	设置超时，以分钟计，范围为 1 到 480。默认的超时设置为 30。
协议支持	设置用户验证时使用的协议： ● HTTP ● 将 HTTP 重新定向到安全通道（HTTPS），如需要重新定向到 HTTPS。 ● HTTPS ● FTP ● Telnet

参数名称	参数说明
证书	如果使用 HTTPS 协议支持，从设置用户验证的下拉菜单中选择“本地证书”。该选项只有在 HTTPS 支持协议被选择后，才可用（包括从 HTTP 重新定向）。默认的设置是“自签”证书。应用 点击“应用”使配置生效。

第24章 反病毒保护

24.1 概述

描述

当您创建防火墙保护文件时，进入反病毒保护菜单访问反病毒配置选项。

内容

24.2 操作顺序

反病毒处理包括各种执行相对独立的各种模块与引擎。ZXSEC US 设备是以基于 web 的管理器菜单中显示的顺序执行该操作的：

- 文件过滤器
- 病毒扫描
- 灰色软件扫描
- 启发性扫描

如果一个文件没有通过以上的操作中的任何一个环节，便不进行接下来的扫描操作。例如，如果文件“fakefile.exe”验证为被屏蔽的文件模式，ZXSEC US 设备将对终端用户发送替换信息且该文件被删除或隔离。病毒扫描、灰色软件或启发式扫描在文件已经被检测认为是具有威胁性或已经被处理的情况下就不执行了，没有必要在已识别的文件上耗费更多的系统资源。

24.3 反病毒操作构成

反病毒的操作是逐项进行的，对通过的文件提供有效的扫描方式。如上所述的前三项操作均具有具体的功能，第四项扫启发式描式目的在于覆盖检测任何新出现的、之前未知的病毒威胁。这四项操作协同执行对网络提供全访问的反病毒防护。为了确保系统能够具有及时的保护，需要定期通过 ZXSEC US 反病毒服务更新所有病毒定义与特征。以下将逐项介绍反病毒的操作，以及 ZXSEC US 反病毒服务。

文件过滤器

文件被接受后，ZXSEC US 设备将对文件模式和文件类型识别过滤操作。ZXSEC US 设备将文件与配置的文件模式和文件类型设置进行匹配查看，如果该文件的文件模式或文件类型属于被屏蔽的模式，例如，EXE，文件传输将被终止且系统会对终端用户发送替换信息进行通知。对该文件也不继续应用其他的扫描程序。如果文件没有被屏蔽，将应用接下来的扫描程序。

病毒扫描

文件在通过文件模式操作后，继续对其应用病毒扫描。病毒定义通过中兴通讯 Distribution Network 保持最新的更新。病毒列表时定期更新的，您不需要等到固件升级。有关更新病毒定义的详细信息，参见“US Service 反病毒保护”。

灰色软件扫描

通过文件模式匹配与病毒扫描操作后，通过的文件流量还要进行灰色软件扫描。灰色软件扫描配置是可以根据需要启动或撤消的，其升级的方式与反病毒定义升级一样。有关配置灰色软件的信息，参见“查看灰色软件列表”。

启发式扫描

当进入的文件流量通过以上所述的三项反病毒操作后，最后还要进行启发式扫描。ZXSEC US 设备启发式扫描反病毒引擎对文件执行测试以检测类似病毒的行为或已知病毒的指示特征。以这种方法，启发式扫描可能检测到新的病毒，但是也可以产生一些误报结果。



注意：

启发式扫描只能适用 CLI 进行配置。参见 ZXSEC US 设备 CLI 使用参考手册。

US Service 反病毒保护

US Service 反病毒服务是出色的资源与服务，包括通过 US Service Distribution Network（US SERVICE 中心）进行病毒与 IPS（攻击）引擎与定义的自动更新以及本地垃圾邮件的 DNSBL。US Service 中心还提供 US Service 病毒与攻击信息列表以及 US Service 公告牌。

ZXSEC US 设备与 US Service 中心的连接是通过进入系统配置>维护>US Service 中心配置的。详细信息，参见“配置 US 设备与 US SERVICE 中心连接与 US Service 服务”。



注意：

如果 ZXSEC US 设备中启动了虚拟域，可以对反病毒功能进行全局配置。在主菜单项中点击“全局配置”可以访问反病毒功能。

24.4 反病毒设置与控制

在整个系统范围内配置使用了反病毒保护的同时，基于每项内容保护列表可以执行具体的设置。表 34 所示是保护内容表中反病毒配置选项与反病毒菜单的比较。

反病毒与保护内容表反病毒配置选项

保护内容表反病毒选项	反病毒设置
病毒扫描	反病毒>配置>病毒列表
启动或撤消对每项流量的病毒扫描（HTTP，FTP，IMAP，POP3 与 SMTP）	查看当前的病毒只读列表。
文件屏蔽	反病毒>文件屏蔽
启动或撤消对于每项流量的文件屏蔽功能。	配置屏蔽所要屏蔽文件的模式，启动或撤消对每项流量的屏蔽功能。
隔离文件	反病毒>隔离
启动或撤消反病毒隔离功能。只在配有本地硬盘的 ZXSEC US 设备可以配置隔离功能。	查看并分类隔离文件列表，配置文件模式自动上传到中兴通讯技术支持进行文件分析并在反病毒中配置隔离选项。
通过分片邮件	启动或撤消通过分片邮件。分片邮件不能够进行病毒扫描。
用户舒适	
启动或中止对 HTTP 与 FTP 流量的用户舒适设置。设置触发用户舒适的时间间隔与容量（byte）。	
超大文件/邮件	

保护内容表反病毒选项	反病毒设置
配置 ZXSEC US 设备屏蔽或通过超大容量的文件与邮件。	
	反病毒>配置>灰色软件
	启动或中止根据类型屏蔽灰色软件。
在外向邮件中添加特征	
创建并启动在外向传输邮件中附加特征标注的功能。（只适用于 SMTP 流量）	

24.5 文件模板

配置文件屏蔽功能将隔离具有潜在威胁的文件，保护计算机设备免受病毒攻击。您可以根据文件的名称，扩展名以及其它文件模式隔离潜在的威胁性的文件。



注意：

文件屏蔽的条目并不是对大小写要求完全匹配的查询。例如，在文件屏蔽列表中添加“.exe”将屏蔽任何以.EXE 结尾的文件。

您可以选择在保护配置中撤消文件屏蔽功能，启动该功能只能够临时性的屏蔽一些具体造成安全性威胁的文件。您可以屏蔽文件的模式，启动或中止文件屏蔽功能。

ZXSEC US 设备将屏蔽与配置的文件模式相匹配的文件并显示以替换信息。您可以配置 ZXSEC US 设备让屏蔽文件的信息保存在病毒日志中并发送报警邮件。

如果同时启动了文件屏蔽与病毒扫描，ZXSEC US 设备将与配置文件模式匹配的文件屏蔽并不会屏蔽的文件实行病毒扫描。



注意：

如果 ZXSEC US 设备中启动了虚拟域，可以对反病毒功能进行全局配置。在主菜单项中点击“全局配置”可以访问反病毒功能。

查看文件模式列表目录

您可以添加多个文件模式列表，然后对每项内容保护列表选择最佳的文件模式。进入反病毒>文件模式，查看文件模式列表。您可以点击列表中每项文件模式列表对应的编辑图标查看详细信息。

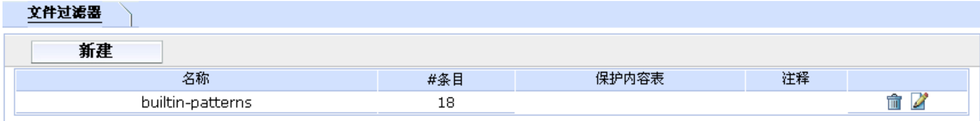


图24.5-1 文件模式列表目录



注意：

默认的文件模式列表目录称为布告模式。

参数信息

参数名称	参数说明
新建	点击“新建”在目录中添加新的文件模式列表。
名称	可用的文件模式列表。
#条目	文件模式列表中文件模式的编号。
内容保护列表	每项文件模式列表应用的内容保护列表。
注释	文件模式列表的描述。
删除图标	从目录中删除文件模式列表。当文件条目列表应用于内容保护列表时不能够被删除。
编辑图标	点击编辑文件模式列表、列表名称或注释。

在内容保护内容保护列表中选择文件模式列表。详细信息，参见“反病毒选项”。

创建新的文件模式列表

进入反病毒>文件模式并点击“新建”将文件模式添加到文件模式列表目录中。

新列表

名称

注释 (最大63个字符)

确定 取消

图24.5-2 新建文件模式列表

参数信息

参数名称	参数说明
名称	输入新建列表名称。
注释	如需要，输入对该列表的描述。

查看文件模式列表

进入反病毒>文件模式查看文件模式列表。

文件过滤器

名称 builtin-patterns

注释 (最大63个字符) 确定

新建

过滤器	操作	启动
文件模式 (18)		
*.bat	阻断	
*.com	阻断	
*.dll	阻断	
*.doc	阻断	
*.exe	阻断	
*.gz	阻断	
*.hta	阻断	
*.ppt	阻断	
*.rar	阻断	
*.scr	阻断	
*.tar	阻断	

图24.5-2 文件模式列表示例

参数信息

参数名称	参数说明
名称	文件模式列表名称。在名称字段点击输入新的名称后点击OK 可以更改文件模式列表的名称。
注释	对文件模式列表添加描述内容。在描述字段添加或编辑描述内容。
新建	点击新建在文件模式列表中添加新的模式。
模式	当前文件模式列表。
动作	对于与文件模式相匹配的流量所采取的动作，屏蔽或允许。
启动	选中栏目中的功能框表示启动该文件模式；相反，中止该文件模式。
删除图标	从列表中删除文件模式。
编辑图标	点击编辑文件模式与动作。
移动图标	将文件模式移动到列表中的任何位置。

ZXSEC US 设备接收到的文件与列表中的文件模式依上而下进行匹配。如果没有发现匹配，该文件将继续进行下一个流程反病毒扫描（如果启动了病毒扫描功能）。如果文件没有被屏蔽将被通过。

如果动作设置为“允许”，除非明确通过这些文件否则文件一直将保持被屏蔽状态。输入所要通过的文件模式以及允许的属性。在列表的末尾，添加表示全部包括的通配符（*.*）并设置采取屏蔽的动作。如果所检测文件与任何文件模式都不相匹配将统一被屏蔽，您可以设置这些文件继续过渡到下一个流程进行反病毒扫描。

文件模式列表预先配置了模式的文件模式列表：

- 可执行文件(*.bat，*.com，以及*.exe)
- 压缩或存档文件(*.gz，*.rar，*.tar，*.tgz，以及*.zip)
- 动态链接库(*.dll)
- HTML 应用程序(*.hta)
- Microsoft Office 文件(*.doc，*.ppt，*.xl?)
- Microsoft Works 文件(*.wps)
- Visual Basic 文件(*.vb?)
- 屏保文件(*.scr)
- 程序信息文件(*.pif)

文件模式将在内容保护中启动。详细信息，参见“反病毒选项”。

配置文件模式列表

文件模式最多可以设置为 80 个字符的长度。列表中的文件模式最多设置 9000 条项目。

在查看文件模式列表时，点击“新建”可以添加新的文件模式。点击每个模式对应的编辑图标可以修改并编辑文件模式条目项。



图24.5-3 新建文件模式

参数信息

参数名称	参数说明
模式	输入文件模式。文件模式可以是精确的文件名称，或是包括通配符的文件模式。
动作	从下拉菜单中选择文件模式类型：通配符或常规表达式。
启动	点击启动文件模式。

24.6 病毒文件隔离

安装有本地硬盘的 ZXSEC US 设备设置隔离被屏蔽与病毒感染的文件。您可以在隔离文件列表中查看文件名称与状态信息。您也可以配置将具体的文件与文件模式添加到自动提交列表中，这些文件将自动上传到中兴通讯公司进行分析。



注意：

如果 ZXSEC US 设备中启动了虚拟域，可以对反病毒功能进行全局配置。在主菜单项中点击“全局配置”可以访问反病毒功能。

24.6.1 查看隔离文件列表

隔离文件列表显示因为病毒感染或文件屏蔽而隔离的文件信息。您可以设置根据文件名、隔离日期、传输形式、状态、DC 或 TTL 其中任何一项对隔离文件进行分类。您也可以过滤隔离文件设置查看具体某一状态的文件或某项服务的文件。

进入反病毒>隔离>被隔离文件，可以查看被隔离的文件列表。

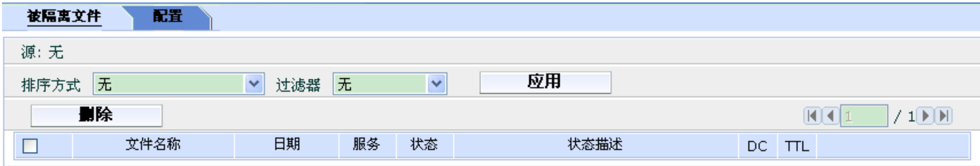


图24.6-1　隔离文件列表

隔离文件列表的功能以及隔离文件信息说明：

参数信息

参数名称	参数说明
应用	点击“应用”将隔离文件分类并过滤。
排序方式	将列表文件进行分类。排序方式：状态、服务、文件名、隔离日期、TTL 或 DC。点击“应用”使排序生效。
过滤器	过滤隔离文件。从状态模式（感染文件，屏蔽文件或启发式检测）或服务（IMAP，POP3，SMAP 或 HTTP）中选择过滤模式。点击“应用”启动过滤服务。启发式模式只能通过 CLI 命令进行配置，参见“反病毒 CLI 配置”。
文件名称	隔离文件处理的文件名称。当文件被隔离，文件名中所包含的空格都将删除，并执行 32 比特的求和校验。存储在 ZXSEC US 硬盘中的文件遵守以下的命名规定：<32bit CRC>.<处理的文件名>。例如，存储名为 Over Size.exe 的文件将被保存为 3fc155d2.oversize.exe.
日期	文件隔离的日期与时间，以月/日/年/时/分表示。如果复制次数增加，该值显示的是文件第一次被隔离的时间。
服务	被隔离文件的传输协议类型。(HTTP，FTP，IMAP，POP3 以及 SMTP)。
状态	文件被隔离的原因：病毒感染，启发式扫描或被屏蔽。
状态描述	与状态有关的具体信息；例如“该文件被 W32/Klez.h 感染”或“文件被文件屏蔽模式阻止”。
DC	复制次数。文件副本被隔离的次数。不断增加的 DC 次数说明一个病毒爆发了。
TTL	激活的时间，以小时/分表示。当 TTL 过期后，ZXSEC US 设备将文件在 TT 标题下标注为 EXP。文件自动复制的情况下，每个复制文件将刷新 TTL。
上传状态	Y 表示文件已经上传到中兴通讯公司进行分析；N 表示文件没有设置自动上传。
删除图标	点击将文件从列表中删除。
下载图标	以其原始格式下载对应的文件。
提交图标	将可疑文件提交到中兴通讯公司进行分析。



注意：

复制的文件（基于校验和）不进行分类，只计数。每发现一个复制的文件，TTL值与复制次数进行更新。

24.6.2 自动提交列表

您可以配置 ZXSEC US 设备将可疑文件自动提交到中兴通讯公司技术支持进行分析。您也可以使用通配符(*或?)将文件模式添加到自动提交列表中。无论文件屏蔽的设置怎样，任何文件模式都可以应用在自动提交列表。

您可以基于文件的状态（被屏蔽的文件或启发式）上传文件或从隔离的文件列表中选择提交单个文件。ZXSEC US 设备通过加密邮件方式通过端口 25 提交到 SMTP 服务器。该功能只应用于安装有本地硬盘的 ZXSEC US 设备。

进入反病毒>隔离区>自动提交列表，查看自动提交列表。

自动提交列表选项

自动列表中的图标及其功能说明：

参数信息

参数名称	参数说明
新建	点击“新建”在自动提交列表中添加新的文件模式。
文件模式	自动上传的文件模式列表。您可是使用？或*通配符创建新的文件模式。选中“启动”功能框启动列表中全部的文件模式。
删除图标	点击将条目从列表中删除。
编辑图标	编辑以下信息：文件模式与启动

24.6.3 配置自动提交列表

进入反病毒>隔离>自动提交列表，将文件模式添加在自动提交列表中。

参数信息

参数名称	参数说明
文件模式	输入自动上传到中兴通讯公司的文件模式或文件名称。
启动	点击启动该文件模式。



注意：

对配置的文件模式启动自动上传功能，您必须进入反病毒>隔离>配置，点击“启动自动提交”以及“使用文件模式”。

24.6.4 配置隔离选项

进入配置设置隔离配置选项包括在不同的服务中设置隔离被屏蔽或病毒感染的文件。您也可以配置 TTL 与文件大小值，以及启动自动提交设置。

隔离设置

选项	HTTP	FTP	IMAP	POP3	SMTP	IM	NNTP
隔离感染文件	☐	☐	☐	☐	☐	☐	☐
隔离可疑的文件	☐	☐	☐	☐	☐	☐	☐
隔离屏蔽文件	☐	☐	☐	☐	☐		☐

时间限制 0 (0-479 小时)

隔离的最大文件大小 0 (0-500 MB)

☐ 日志服务 [配置]

应用

图24.6-2 隔离配置（适用于安装有本地硬盘的 ZXSEC US 设备）

隔离配置的选项参数信息

参数名称	参数说明
选项	隔离感染文件：选择隔离以哪一项协议传输的反病毒扫描识别为受感染文件。 隔离可疑文件：选择隔离以哪一项协议传输的启发式扫描识别为可疑文件。 隔离屏蔽文件：选择隔离以哪一项协议传输的反病毒文件屏蔽功能设置阻止的文件。对于 HTTP 与 FTP 流量，隔离屏蔽文件选项不生效因为一个文件名在下载之前就被屏蔽，当然就不能进行隔离。
时间限制	隔离文件保存的时间期限。保存期限用于计算隔离文件列表中 TTL 栏目的值。当过了保存期限，隔离文件列表中 TTL 项中显示 EXP。隔离文件将被删除。设置保存期限为 0 表示根据设置硬盘的存储容量会对存储的文件采取不同的动作。

参数名称	参数说明
隔离的最大文件的大小	隔离文件的最大值（以 MB 计）。设置隔离文件的最大值。文件太大影响系统性能。
磁盘空间不足	硬盘已满时对隔离的文件采取的动作：覆盖最原始的文件或丢弃新文件。
启动自动提交	启动自动提交功能。选择以下选项： 使用文件模式：启动自动上传与自动提交列表中相匹配的文件模式。 使用文件状态：启动根据文件状态自动上传隔离的文件。 可选的文件状态为：启发式或屏蔽模式。 启发式只有通过 CLI 命令配置启动。参见“CLI 配置”。
应用	点击“应用”保存设置。



注意：

暂时不支持 NNTP 选项。

24.7 配置

配置显示被 ZXSEC US 设备屏蔽的病毒列表。您也可以配置屏蔽超过设置大小的文件与邮件以及灰色软件。



注意：

如果 ZXSEC US 设备中启动了虚拟域，可以对反病毒功能进行全局配置。在主菜单项中点击“全局配置”可以访问反病毒功能。

24.7.1 查看病毒列表

病毒列表以字母顺序显示屏蔽的病毒列表（也称为 AV 定义）。您可以通过选择编号或字母范围查看全部或部分病毒列表。ZXSEC US 设备使用病毒定义检测并移除通过 ZXSEC US 的内容流量中携带的病毒、蠕虫、特洛伊木马以及其他威胁。

进入反病毒>配置，查看病毒列表。

US Service 病毒定义列表在每次 ZXSEC US 设备接收到新的 AV 定义时进行更新。

US Service 中心病毒信息大全中 ZXSEC US 设备可以检测到的病毒、蠕虫、特洛伊木马以及其他网络威胁的信息描述。

病毒列表　灰色软件

0 - 9　A - F　G - L　M - R　S - Z　All

ActivCrk.A!tr	AdClck!tr	AdClicker.C!tr
AdClicker.D!tr	AdClicker.G!tr	AdClicker.H!tr
AdClicker.P!tr	Agent.AF!tr	Agent.AI!tr
Agent.AK!tr.spy	Agent.B!tr	Agent.BF!tr.spy
Agent.BV!tr.spy	Agent.BW!tr.spy	Agent.CF!tr.spy
Agent.CK!tr.spy	Agent.DEK!tr	Agent.FWP!tr
Agent.FXQ!tr	Agent.GCK!tr	Agent.GCY!tr
Agent.GDP!tr	Agent.GEU!tr	Agent.GGJ!tr
Agent.GHJ!tr	Agent.GIU!tr	Agent.GJE!tr
Agent.GKX!tr	Agent.K!tr.dldr	Agent.P!tr.dldr
Agent.R!tr.dldr	Agent.S!tr	Agent_ba.E!tr.spy
Agent_cj.B!tr.spy	Agent_cj.C!tr.spy	Agent_cj.D!tr.spy
Agent_cj.H!tr.spy	Agent_cj.J!tr.spy	Agent_cj.K!tr.spy
Agent_cj.M!tr.spy	Agent_cj.N!tr.spy	Agent_cj.P!tr.spy
ALS/Bursted	Aluigi!exploit	Ambler.A!tr
ANP!tr.pws	Antav.A!tr.spy	AntiCMOS.fam
Antilam.AJW!tr	ANU.CE!tr.pws	AOW!tr.pws
APA!tr.pws	APJ!tr.pws	APS!tr.pws
Ardamax!tr.klog	Ardamax.N!tr	AzeSearch!tr
Backdoor!tr	BackDoor.AC!tr	BackDoor.B!tr

图24.7-1　病毒列表（部分）

通常情况下，US Service AV 定义是通过 ZXSEC US 设备与 US SERVICE 中心（FortiGuard Distribution Network）的连接自动获取的。进入系统配置>维护>US Service 中心，配置从 US SERVICE 中心自动获取 AV 定义更新。

您也可以在系统面板中（进入系统配置>状态）设置手动更新 AV 定义。

24.7.2 查看灰色软件列表

灰色软件程序是没有经过用户允许，安装在用户计算机设备的带有商业性的目的的软件程序。灰色软件通常令人讨厌并且这些程序可能导致系统功能问题或用于恶意的目的或手段。

ZXSEC US 设备可以扫描已知的灰色软件可执行程序。每当 ZXSEC US 设备接受到病毒更新数据包时将更新类型列表与内容。新的类型可以在任何时间添加并加载病毒更新。默认的情况下，所有的新类型都是没有启动。当启动病毒扫描时保护内容表中将启动灰色软件扫描程序。

灰色软件都是由已知的可执行文件构成。每当 ZXSEC US 设备接收到一个病毒与攻击定义更新，灰色软件类型与内容也随之进行更新。



注意：

如果 ZXSEC US 设备中启动了虚拟域，可以对反病毒功能进行全局配置。在主菜单项中点击“全局配置”可以访问反病毒功能。

进入反病毒>配置>灰色软件，查看灰色软件列表。

病毒列表 灰色软件

类别	启用
Adware	☐
BHO	☐
Dial	☐
Download	☐
Game	☐
HackerTool	☐
Hijacker	☐
Joke	☐
Keylog	☐
Misc	☐
NMT	☐
P2P	☐
Plugin	☐
RAT	☐
Spy	☐
Toolbar	☐

图24.7-2 灰色软件选项

程序类型随着 ZXSEC US 设备接收更新可能会更改或扩展。在上图所示的列表中您可以选择启动以下灰色软件类型。启动灰色软件类型屏蔽类型列表中所列的全部文件。

参数信息

参数名称	参数说明
Adwear（广告软件）	启动屏蔽 adware 软件程序。Adware 通常嵌在一些免费的程序中，当使用或打开这些免费程序时将弹出广告页面。
Dial（自动拨号程序）	启动屏蔽自动拨号程序。自动下载并安装到用户的计算机上，并隐藏在后台运行。它会自动拨打长途或收费电话，以赚取用户高额的电话费用。
Game（游戏程序）	启动屏蔽下载游戏程序。这些游戏程序通常是一些网络笑话或无聊网络游戏，您可以设置屏蔽这些程序。
Joke（玩笑程序）	启动屏蔽玩笑程序。一个会导致各种各样的良性行为显示在你电脑上的无害程序（例如一个不期望出现的屏幕保护程序）。
P2P（点对点程序）	启动屏蔽点对点通讯程序。点对点传输协议是合法的网络协议，类似文件共享程序；通常用于非法的交换音乐，电影与其它文件等。
Spy（间谍程序）	启动屏蔽间谍程序。是一种能够在用户不知情的情况下，在其电脑上安装后门、收集用户信息的软件。
Keylog（键盘记录器程序）	启动屏蔽键盘记录器程序。该程序通过挂系统键盘钩子等方式记录键盘输入，从而窃取用户的帐号、密码等隐私信息。
Hacker 工具	屏蔽 hacker 工具。
Hijacker（浏览器劫持程序）	启动屏蔽浏览器劫持程序。是一种恶意程序，通过浏览器插件、BHO（浏览器辅助对象）、Winsock LSP 等形式对用户

参数名称	参数说明
	的浏览器进行篡改，使用户的浏览器配置不正常，被强行引导到商业网站。
Plugin（插件程序）	启动屏蔽浏览器插件程序。浏览器插件通常是一些无害的互联网浏览工具，可以从流量器窗口直接安装与操作。一些工具栏与插件试图控制或记录以及发送浏览参数。
NMT（网络管理工具）	启动屏蔽网络管理工具程序。它是自动安装的用于恶意更改网络设置并干扰网络安全的程序。
P2P	屏蔽 P2P 通信程序。P2P 虽然是合法的协议，但是经常被非法用于交换电影、音乐以及其他文件。
RAT（远程管理工具）	启动屏蔽远程管理工具程序。远程管理工具程序允许外部用户远程操作并监控网络中的计算机设备。
Misc（恶意程序）	启动屏蔽各种灰色软件程序。
BHO（IE 插件）	启动屏蔽 IE 插件程序。IE 插件是嵌入软件包作为其一部分进行安装的 DLL 文件,它可以控制 IE4 版本或更高版本 IE 浏览器的行为。并不是所有的 BHO 都是恶意的程序，但是这些程序潜伏在设备中跟踪用户的网页浏览习惯并搜集其它信息。
Toolbar（工具栏程序）	启动屏蔽工具栏程序。虽然一些工具栏程序是无害的，但是间谍软件的开发人员可以使用这些工具栏监控用户网页浏览的习惯等。
Download（下载程序）	启动屏蔽下载程序。下载部件通常在 Windows 启动时自动运行并设计安装或下载其它软件程序，特别是一些广告以及自动拨号软件程序。

24.8 反病毒 CLI 配置命令

本手册只对基于 web 管理器中没有对应的操作以及配置选项的命令行接口（CLI）命令，关键词或变量（斜体）进行了描述。有关全部的 CLI 命令及其用法，参见 ZXSEC US 设备 CLI 使用参考手册。

系统全局优化

系统全局优化功能配置 CPU 设置确保 ZXSEC US 设备有效的执行反病毒扫描或信息吞吐量。当对反病毒功能启动了优化功能后，ZXSEC US 设备使用均衡多处理技术将反病毒扫描任务分散到几个 CPU，加快了扫描速度。

有关反病毒失效开放与优化功能的详细信息，参见中兴通讯知识库。

config antivirus heuristic

ZXSEC US 启发式反病毒引擎对文件执行病毒扫描，检测类似病毒的行为特征或作病毒源程序分析。启发式病毒扫描在文件屏蔽与病毒扫描操作结束没有发现任何匹配结果时启动。在此情况下，启发式扫描可能会检测到新的病毒，但也可能产生一些病毒误报结果。

当传输到收件人的邮件被怀疑是病毒文件时，启发式病素扫描程序就会启动并发送文件隔离通知给收件人。在 CLI 配置操作中，启动病毒扫描时保护内容列表中的启发式病毒扫描也随之启动。

使用相关命令更改启发式扫描模式。

config antivirus quarantine

隔离命令也可以配置允许启发式病毒扫描有关的设置。

config antivirus service<service_name>

使用该命令配置 ZXSEC US 设备在 http、FTP、IM、POP3、IMAP 或 SMAP 流量中如何处理超大容量文件的反病毒扫描以及对 http 流量配置端口执行病毒扫描。

第25章 IPS（入侵防护保护）

25.1 概述

描述

ZXSEC US 入侵防护系统（IPS）将特征与异常入侵防护结合，降低了威胁的潜伏期，增强了设备的可靠性。创建防火墙保护内容列表同时可以配置 IPS 选项。

内容

25.2 关于入侵防护保护

ZXSEC US 设备将可疑流量进行日志记录，并给系统管理员发送报警邮件。您可以对可疑数据包或会话采取日志记录、允许通过、丢弃会话、重置会话或清除动作。调一些 IPS 异常阀值与保护网络中的正常流量配合操作。您还可以创建 ZXSEC US IPS 用户定义特征应对不同的网络环境。

ZXSEC US IPS 入侵防护功能是将网络流量模式与攻击特征库中的特征相匹配。攻击特征检测保护您的网络不受到已知的攻击造成损失。

ZXSEC US 设备与 US Service 服务器的连接是通过进入系统配置>维护>US Service 中心配置的。详细信息，参见“配置 ZXSEC US 设备与 US Service 服务”。

您可以配置 ZXSEC US 设备自动检查并下载或手动下载包含有最新特征的文件以便更新攻击特征。

当 ZXSEC US 设备安装了更新的攻击定义文件后，将查看任何现有的特征的配置是否发生更改。如果默认的配置发生更改，更改信息将被保留。

除了拥有庞大的预先定义的攻击特征列表外，您还能够创建用户自定义攻击特征列表。

IPS 检测或防止攻击的同时将生成攻击信息。您可以配置 ZXSEC US 设备将生成的信息添加到攻击日志并发送报警邮件给系统管理员。以及配置 ZXSEC US 设置发送报警邮件的频率。您还可以通过撤消对那些系统中没有使用的程序所定义的特征，减少日志信息与报警信息的数量。（例如，您没有运行 Web 服务器，那么有关定义给 Web 服务器的 Web 攻击特征就可以取消）。

数据包日志记录使管理员能够对数据包的合法性以及是否误报进行分析。

有关 ZXSEC US 设备日志记录以及报警邮件的信息，参见“日志与报告”。

您可以使用基于 web 的管理器或 CLI，配置 IPS 功能，分别在每项内容保护列表中启动或中止所有的特征或异常检测。



注意：

如果 ZXSEC US 设备中启动了虚拟域，可以对 IPS 功能进行全局配置。在主菜单项中点击“全局配置”可以访问 IPS 功能。

IPS 的使用

IPS 系统最适合于大型网络以及保护网络中的高敏感信息。通过监视和分析攻击日志，确定攻击的性质以及威胁等级，这样能够更有效的使用 IPS 系统。管理员通过调整阈值在入侵防护与系统性能之间把握最佳的平衡点。

25.3 预定义的特征

预定义的特征基于攻击类型分组。默认情况下，并不启动所有特征，而是启动记录了所有特征的日志。检查默认的设置确保定义的特征与网络的流量类型相符合。

仅使用您需要的特征检查，可以提高系统性能，并减少日志记录的数量与 IPS 生成的报警邮件。例如，ZXSEC US 的 IPS 可以检测大量针对 Web 服务器的攻击，如果您并没有 Web 服务器需要 ZXSEC US 设备保护，那么您可以撤消全部的 Web 服务器攻击特征以提高系统性能。



注意：

如果 ZXSEC US 设备中启动了虚拟域，IPS 功能在每一个虚拟域中单独配置。所有的传感器和用户定义特征尽属于创建时所在的虚拟域中。

25.3.1 查看预先定义的特征列表

您可以在预先定义的特征列表中启动或中止预先定义特征组并配置单个预先定义特征的设置。该列表是根据特征的危险级别进行排列的。



注意：

如果 ZXSEC US 设备启动了虚拟域设置，IPS 功能项可以通过全局配置进行设置。

进入入侵防护>特征>预定义，可以查看预先定义的特征列表。

预定义 | 定值 | 协议解码器

1 / 58 [列设置] [清除所有的过滤条目]

名称	严重性	对象	协议	OS	应用程序	启用	行为
2BGal.Disp_album.SQLInjection	低	服务器	TCP, HTTP	All	PHP_app		通过
3Com.3CDaemon.FTP.Server.Information.Disclosure	低	用户端	TCP, FTP	Windows	Other		通过
3COM.OfficeConnect.DoS	低	服务器	TCP, HTTP	Other	Other		丢弃
8Pixel.net.SimpleBlog.SQL.Injection	高	服务器	TCP, HTTP	All	Other		通过
A1stats.A1disp.DirectoryTraversal	高	服务器	TCP, HTTP	Linux	CGI_app		丢弃
AA.bot.Botlist.File.Access	低	服务器	TCP, HTTP	Windows	Other		通过
Aardvark.Topsites.PHP.Arbitrary.Command.Execution	中	服务器	TCP, HTTP	All	PHP_app		通过
Aardvark.Topsites.PHP.Remote.Command.Execution	中	服务器	TCP, HTTP	All	PHP_app		通过

图25.3-1　预先定义的特征列表

默认特征列表按照名称排序，可以通过单击相应列的列头改为按照此列排序。

参数信息

参数名称	参数说明
列设置	可以修改特征列表显示的列以及列的顺序。
清除所有的过滤条目	清除所有的特征显示过滤条件。
名称	特征的名称。
严重性	每项特征的危险级别设置。这些级别可以设置为信息、低、中、高以及危险。
对象	每项特征保护的对象，有保护服务器的特征，也有保护客户端的特征，或者两者都保护的特征。
协议	每项特征所针对的网络协议。
OS	每项特征所保护的操作系统。
应用系统	每项特征所保护的应用系统。
行为	每项特征的默认行为：通过或丢弃。 “通过”表示不对网络流量做任何处理。如果您希望测定

参数名称	参数说明
	IPS 特征对网络的影响，可以设置启用相应的特征，将特征的行为设置为“通过”，并启用日志。您可以通过详细的检查日志来了解相应的特征而不会影响网络流量。 “丢弃”表示对符合特征的网络流量进行保护。如果启用日志，行为会显示在日志数据的状态字段中。
ID	每项特征唯一的数字标识。
启用	特征的状态显示。对应特征的“启用”显示为打勾状态时表示该特征已启用。相反，对应特征的“启用”显示为灰色打叉状态时表示没有启用。
日志	特征的默认日志行为。打勾状态表示该特征已启用日志。相反，显示为打叉状态时表示没有启用日志。
组	每项特征都属于一个组。组仅用于分类特征，便于管理，不用于特征过滤器。
数据包日志	每项特征默认的数据包日志状态。打勾状态表示该特征已启用日志。相反，显示为打叉状态时表示没有启用日志。
修正	每项特征的修正版本。当某项特征更新时，则此特征的修正版本号相应增加。

使用显示过滤器

默认特征列表显示所有的预定义特征，可以使用过滤器只显示您关注的特征。如您想浏览只与 Windows 系统相关的特征，可以设置 OS 过滤条件。通过单击每列名称旁边的过滤器图标，设置相应的过滤条件。

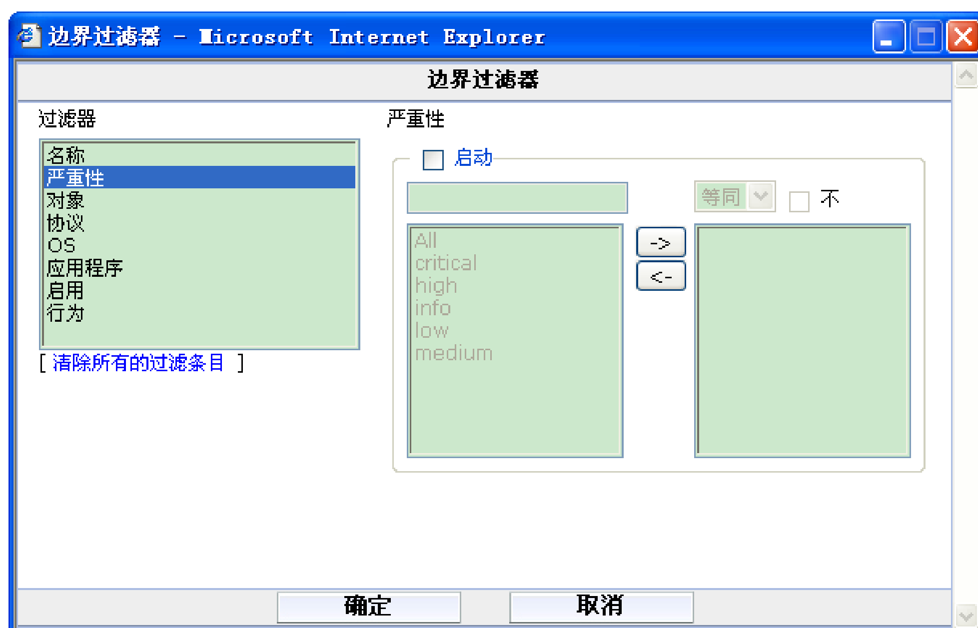


图25.3-2　使用显示过滤器

25.3.2 调整预先定义的特征加强系统性能发挥

默认情况下，ZXSEC US 设备将启动大多数预先定义的特征并对这些特征进行日志记录。根据您的网络配置请求，您可以调整这些特征设置。通过调整特征与日志设置，您既可以配置可用的最佳网络保护设置又可以获得更高的 ZXSEC US 设备性能。调整特征允许您将不使用的功能关闭。关闭不使用的特征与这些特征的日志纪录功能，ZXSEC US 设备便释放了更多资源更快的处理程序任务提高整个系统的性能。

并不是所有的系统都需要进行全部特征扫描。例如，您配置的网络中 ZXSEC US 设备只控制网络中计算机访问内部数据库，但不访问互联网或邮件，那么便没有必要配置 ZXSEC US 设备对一些特征类型，如邮件、IM 与 P2P 进行扫描。

配置 ZXSEC US 设备不查询这些特征，便可以保持较高级别的安全性的同时增强了整体的性能。

准确查看日志功能所产生的日志信息有助于增强网络的安全性。如果您发现这些日志信息没有必要，完全可以关闭日志功能。日志是提供行动措施的最好信息来源。

25.4 用户定义特征

用户定义特征功能增强了针对不同的网络环境定义 ZXSEC US IPS 特征的灵活性。ZXSEC US 预先定义的特征覆盖通常情况下的攻击。如果您使用特殊的程序或不同的平台，您可以基于程序与系统平台供应商规定的安全报警级别添加用户定义的特征。

您也可以通过自定义特征来阻断特定的 P2P 应用。



注意：

如果 ZXSEC US 设备中启动了虚拟域，IPS 功能在每一个虚拟域中单独配置。所有的传感器和用户定义特征尽属于创建时所在的虚拟域中。

25.4.1 查看用户定义特征列表

进入入侵防护>特征>定制，查看用户定义的特征列表。

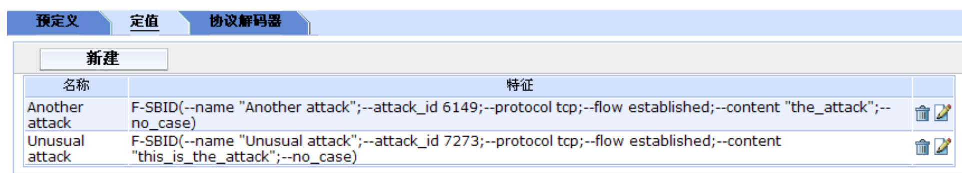


图25.4-1　用户定义特征组

25.4.2 创建用户定义的特征

使用用户定义的特征可以屏蔽或允许一些具体特征项的流量。例如，可以屏蔽含有色情类信息的流量，创建如下的用户定义特征：

set signature 'F-SBID (--protocol tcp; --flow bi_direction;--pattern "nude cheerleader"; --no_case)'

有关用户定义特征句法的详细信息，参见 ZXSEC US 设备入侵防护保护系统（IPS）使用手册。



注意：

用户定义特征是高级功能。本手册说明的出发点将站在具有一定创建入侵防护特征的用户角度进行阐述。

进入入侵防护>特征>定制，创建用户定义的特征。

新建用户定制特征

名称

特征

确定 取消

图25.4-2 编辑用户定义的特征

参数信息

参数名称	参数说明
名称	用户定义特征的名称。
特征	输入用户定义的特征。有关用户定义特征句法的详细信息，参见 ZXSEC US 设备入侵防护保护系统（IPS）使用手册。

25.5 协议解码器

ZXSEC US 设备的 IPS 系统采用协议解码器来识别不符合协议标准的非正常网络流量模式。如 HTTP 解码器监视和识别 HTTP 数据包是否符合 HTTP 的协议标准。

在解码器列表中您可以看到所有解码器以及解码器检测的端口号。

查看协议解码列表

进入入侵防护>特征值>协议解码器，查看解码列表。

预定义 定值 协议解码器

协议	端口
Back Orifice	自动
DCE RPC	135, 1026
DNS	53
FTP	21
H323	1720
HTTP	自动
Instant Messaging	自动
IMAP	143
LDAP	389
MSSQL	1433
NetBIOS	139, 445
Peer-to-Peer	自动
POP3	110
Protocol (L3/4) Analyser	自动
RADIUS	1812,1813
Sun RPC	111, 32771
SIP	自动
SMTP	25
SNMP	161, 162
SSH	自动
TCP Reassembler	自动
TFN DoS	自动

图25.5-1 协议解码列表

25.6 IPS 传感器

为了更方便的选择保护内容表，在 IPS 传感器中加入了特征组。具有特定类型流量的特征被分别定义为单独的 IPS 传感器，在内容表中可以选择这些传感器。例如，所有 Web 服务器相关的特征可以定义为一个 IPS 传感器，这个传感器可以作为防火墙策略的保护内容表，ZXSEC US 设备通过此防火墙策略可以控制所有进出 Web 服务器的流量。

预定义的特征可以通过 US Service 服务来进行升级，升级后将增加新的威胁特征。

25.6.1 查看 IPS 传感器列表

进入入侵防护>IPS 传感器查看 IPS 传感器。

IPS 传感器

新建

名称	注释
all_default	all predefined signatures with default setting
all_default_pass	all predefined signatures with PASS action
protect_client	protect against client-side vulnerabilities
protect_email_server	protect against EMail server-side vulnerabilities
protect_http_server	protect against HTTP server-side vulnerabilities

图25.6-1 IPS 传感器清单列出了默认定义的传感器

IPS 传感器清单包含以下信息：

参数信息

参数名称	参数说明
新建	选择增加一个新的 IPS 传感器。
名称	每个 IPS 传感器的名称。
注释	对 IPS 传感器的描述。
删除图标	删除 IPS 传感器。
编辑图标	打开 IPS 传感器并编辑。

默认配置中提供了五个 IPS 传感器。

- all_default

  包含所有特征。设置传感器，使用每个特征的默认启用设置和默认动作。

- all_default_pass

  包含所有特征。设置传感器，使用每个特征的默认启用设置，但动作设置为通过。

- protect_client

  这种传感器仅包括为发现对客户端的攻击而设计的特征。设置传感器，使用每个特征的默认启用设置和行为。

- protect_email_server

  这种传感器仅包括检测针对 SMTP，POP3，或 IMAP 协议的服务的攻击的特征。设置传感器，使用每个特征的默认启用设置和默认动作。

- protect_http_server

  这种传感器仅包括检测针对使用 HTTP 协议的服务的攻击的特征。设置传感器，使用相应特征的默认启用设置和行为。

25.6.2 增加一个 IPS 传感器

在传感器被设置之前必须，通过增加过滤器和跳过的方式创建一个 IPS 传感器。使用以下步骤创建一个新的 IPS 传感器。

图25.6-2 新的 IPS 传感器

1. 进入入侵防护>IPS 传感器
2. 选择“新建”
3. 输入新 IPS 传感器的名称
4. 给新的 IPS 传感器添加一个注释，虽然注释是任意的，当查看传感器列表时，一个简短的描述将有助于区别多个 IPS 传感器。
5. 选择“确定”进入 IPS 传感器配置界面。

25.6.3 配置 IPS 传感器

每个 IPS 传感器由两部分组成；过滤器和跳过。跳过在过滤器前被检查。

每个过滤器由许多特征属性组成。所有的特征都带有这些属性。只有这些属性在过滤器运行的时候被检查。如果多个过滤器定义在一个 IPS 传感器中，则按照从顶部到底部的顺序检查每个过滤器。如果发现有匹配的过滤器，就会采取过滤器中设置的动作，同时不再进行下一个过滤器的检查。

跳过的特征可以修改过滤器中的特征行为，也可以自定义跳过特征。

首先使用跳过的特征检测网络流量，如果没有发现匹配的流量，然后再按照从上到下的顺序调用过滤器列表，使用每一个过滤器中的特征检测网络流量。如果没有匹配任何特征，IPS 传感器不影响网络流量。

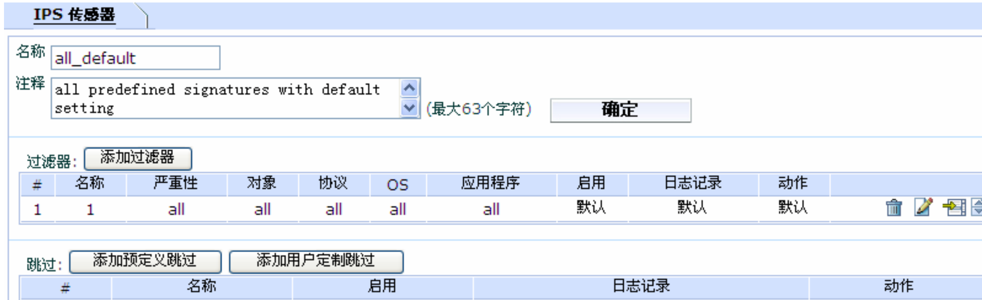


图25.6-3　编辑 IPS 传感器

进入入侵防护>IPS 传感器，点击任意 IPS 传感器的编辑图标。IPS 传感器窗口被分成三部分：传感器属性，过滤器和跳过的特征。

IPS 传感器属性参数信息

参数名称	参数说明
名称	IPS 传感器名称。任何时候都能修改。
注释	对 IPS 传感器的描述。

IPS 传感器过滤参数信息

参数名称		参数说明
添加过滤器		在过滤器列表的后面添加新的过滤器。
#		每个过滤器在列表上现在的位置。
名称		过滤器的名称。
属性	严重性	被包括的特征的严重性。
	对象	被攻击对象的系统类型。对象是客户机或服务器。
	协议	其中特征适用于这些协议。例如包括 HTTP，POP3，h323，和 DNS。
	OS	特征适用的操作系统。
	应用程序	特征适用的应用程序
配置	启用	包括“接收特征的默认配置”、“启用全部”、“禁止全部”。
	日志记录	包括“接收特征的默认配置”、“启用全部”、“禁止全部”
	动作	包括“接收特征的默认配置”、“通过全部”、“屏蔽全部”、“重置全部”
	删除图标	删除过滤器
	编辑图标	编辑过滤器
	插入图标	创建新的过滤器并且将之插入在当前过滤器的上面。
	移动图标	移动目前过滤器。在出现的窗口中，输入清单目的地位置并选择“确定”。

IPS 传感器跳过参数信息

参数名称	参数说明
增加预定义	依据预定义的特征创建一个跳过。
增加自定义	依据自定义的特征创建一个跳过。
#	在每个跳过列表的当前位置。
名称	特征的名称。
启用	跳过的状态被显示出来。绿色圈表明跳过被启用。灰色圈表明跳过没有被启用。
日志记录	跳过的日志记录状态被显示出来。绿色圈表明日志被启用。灰色圈表明日志没有被启用。
动作	跳过的动作设置被显示出来。动作可以被设置成通过，阻止或重新设置。
删除图标	删除过滤器。
编辑图标	编辑过滤器。

25.6.4 配置过滤器

编辑一个过滤器，进入入侵防护>IPS 传感器并选择包含你想编辑的过滤器的 IPS 传感器的编辑图标。当传感器窗口被打开，选择你想更改的过滤器的编辑图标。通过选择五个特征属性，你可以选择包含在一个过滤器中的特征。

- 严重性表示每个特征的级别，严重的特征表示最具危险的攻击，而这些被定为信息的信息具有最低的威胁。五个严重等级级别，从最高到最低，分别是：至关重要的，高，中，低，信息。
- 目标显示了攻击锁定的系统类型。选择是服务器或客户端。
- 协议规定了攻击运用的网络协议。
- OS 列出了容易受到攻击的操作系统。
- 应用清单列出了容易受到攻击的应用程序或应用程序组。

过滤器中的特征包含所有与过滤器属性设置相匹配的特征。

当创建过滤器的时候，将一个新的过滤器的每个属性设置为"ALL"。即所有特征被包含在过滤器中。如果严重性被改为高，而且对象被改为服务器，过滤器就只对服务器上最优先级别的攻击做特征检测。



注意：

如果你不能确定你构造的哪些特征被包含在过滤器中，你可过滤具有相同属性的特征清单。经过滤的清单将显示所有与你指定的属性相匹配的特征。

图25.6-4 编辑 IPS 过滤器

这五个属性中的每一个，你可以选择“全部”或“指定”。选择“指定”则可让您选择相应的选项。

具有 OS ALL 属性的特征不特指某个操作系统，而是涉及所有操作系统。这些特征将被自动列入到过滤器中，一个单一的，多个的，或所有的操作系统都被规定在这些过滤器中。

每个预定义的特征，也具有一个默认启用属性。这个默认显示在特征清单中。当配置一个过滤器时，你可以选择接受这个默认属性或跳过这个属性，为过滤器中包含的所有特征设置启用或禁用。

特征动作的工作方式是相同的，包括默认、全部通过、全部阻断或全部重置。

25.6.5 配置预定义或定制跳过

编辑一个预定义或定制跳过，进入入侵防护>IPS 传感器并选择你打算编辑的有跳过的 IPS 传感器的编辑图标，当传感器窗口打开，选择你打算更改的跳过编辑图标。

配置预定义和定制跳过，以同样的方式运行。

不同于过滤器，每个跳过定义一个特征的行为。

通过跳过可实现 3 个结果：

- 一个特征跳过能改变已包括在一个过滤器中的一个特征的行为，比如，如果你希望保护一个网络服务器，你可以生成一个过滤器，它包括和启动所有和服务器有关的特征。如果你不许可这些特征中的一个，最简单的方法莫过于生成一个跳过并标识该特征无效。
- 一个跳过可以添加一个单独的不包括在任何过滤器中的特征，对于一个 IPS 过滤器。这是唯一能被添加到 IPS 传感器的定制特征的途径。
- 一个特征跳过能用于定义一个依靠流量源和目的文件的特征工作路径。跳过配置许可你指定源和目标 IP 地址或子网络。如果一个地址域是空白的，将包括所有假定地址。

配置IPS跳过

特征

启用

动作 通过

日志记录

数据包日

免除IP

源地址 目标地址

Add

#	源地址	目标地址	

确定 取消

图25.6-5 配置 IPS 跳过

当一个预定义特征在一个跳过中被指定，默认状态和动作属性无效。当生成一个跳过时，必须明确配置这些设置。

25.7 DoS 传感器

ZXSEC US 设备的 IPS 通过异常检测机制来识别不符合已知或常规流量模式和行为的网络流量。比如一种 flooding 的 DoS（拒绝服务）攻击，是指攻击源向目标系统发出大量的连接请求，导致减缓甚至迫使目标系统停止运行，从而合法用户也无法使用目标系统。这就是 DoS 传感器名称的起源，但实际 DoS 传感器可防御很多异常攻击。

Dos 传感器可以设置是否记录流量异常日志，可以设置检测阀值，并在超过检测阀值时启用设置的动作。

可创建多个 DoS 传感器。每个传感器依次检查网络流量，从头至尾。当一个传感器检测到异常，则启用已设置的动作。因为每个传感器都可配置为从一个特定地址，一个特定端口或任何组合中检测流量，所以在检测异常时，多传感器具有更细的粒度。

当设置 DoS 传感器时，适配范围最小的传感器放置在最上方，适配范围最大的传感器在最下方。比如，一个没有指定被保护地址和端口的传感器匹配所有流量。如果该传感器在列表上方，后面的传感器都不执行。

仅在 ZXSEC US 设备固件更新时，会更新 DoS 异常检测类别。



注意：

如果 ZXSEC US 设备设置了虚拟域，每个虚拟域有自己的入侵防设置，包括传感器和自定义特征。

ZXSEC US 设备的 IPS 通过异常探测去定义不符合已知或常规流量模式和行为的网络流量。比如一种 flooding 是 DoS 攻击，发生在当一个攻击系统启动有目标系统的一个异常高会话数时。高会话数减缓或目标系统停止运行，因此合法用户不再能使用目标系统。该攻击通过对大量异常攻击的探测和保护性能为 DoS 传感器命名。

记录或不记录每个流量异常，配置检测阀值并在超过检测阀值时启用设置的动作。

可创建多个 DoS 传感器。每个传感器依次检查网络流量，从头至尾。当一个传感器检测到异常，则应用配置的动作。因为每个传感器都可配置为从一个特定地址，一个特定端口和任何组合中检测流量，所以在检测异常时，多传感器具有很大粒度。

当设置 DoS 传感器时，最特殊的传感器放置在最上方，最普通的在最下方。比如，一个没有指定的被保护地址和没有指定端口的传感器匹配所有流量。如果该传感器在列表上方，后面的传感器都不执行。

流量异常检测列表仅在 ZXSEC US 设备软件被更新时才得以更新。

注意：

如果 ZXSEC US 设备设置了虚拟域，入侵防护在每个虚拟域中设置，所有传感器和特征仅出现在创建的虚拟域中。

25.7.1 查看 DoS 传感器列表

进入入侵保护>DoS 传感器查看异常列表

DoS 传感器

新建

状态	ID	名称	注释	
☐	1	testDos		

图25.7-1 DoS 传感器列表

参数信息

参数名称	参数说明
新建	在列表的底端生成一个新的 DoS 传感器
状态	选中则启动 DoS 传感器，否则停止 DoS 传感器
ID(标识)	仅作为 DoS 传感器的唯一标识符，与 DoS 传感器在列表中的顺序无关。
名称	DoS 传感器名。
注释	对 DoS 传感器的描述。
删除	选择删除 DoS 传感器。
编辑图标	选择编辑下列信息：Action， Severity，Threshold。
插入 DoS	选择在当前传感器前生成一个新的 DoS 传感器。
移动图标	移动当前 DoS 传感器在列表列表中的位置。

25.7.2 配置 DoS 传感器

由于一个配置不恰当的 DoS 传感器可能阻挡网络流量，在默认配置中，没有设置 DoS 传感器，同样，新创建的传感器默认不启动，并预设了默认阀值，通过调整默认阀值来满足您的网络需求。



注意：

在改变默认阀值前请了解正常和预期的网络流量。阀值设定的太低会阻挡正常的流量，阀值设定的太高，会遭受本可避免的攻击。

配置 DoS 传感器，进入入侵防护>DoS 传感器选择现有 DoS 传感器的编辑图标，或选择“新建”生成一个新的 DoS 传感器。

DoS 传感器

新DoS传感器

名称

注释 (最大63个字符)

异常配置：

名称	启动	日志记录	动作	阀值
tcp_syn_flood	☐	☑	通过	2000
tcp_port_scan	☐	☑	通过	1000
tcp_src_session	☐	☑	通过	5000
tcp_dst_session	☐	☑	通过	5000
udp_flood	☐	☑	通过	2000
udp_scan	☐	☑	通过	2000
udp_src_session	☐	☑	通过	5000
udp_dst_session	☐	☑	通过	5000
icmp_flood	☐	☑	通过	250
icmp_sweep	☐	☑	通过	100
icmp_src_session	☐	☑	通过	300
icmp_dst_session	☐	☑	通过	1000

受保护地址：

目标地址	目标端口	源地址	
0.0.0.0/0	0	0.0.0.0/0	添加

图25.7-2 编辑 DoS 传感器

DoS 传感器属性参数信息

参数名称	参数说明
名称	DoS 传感器名

参数名称	参数说明
注解	DoS 传感器的一个可选描述。该描述将出现在 DoS 传感器列表使每项更容易明白含义。

DoS 传感器异常配置参数信息

参数名称	参数说明
名称	异常的名称
启用	是否启用
日志	当被选择时，当异常发生时 DoS 传感器将记录日志，标题行的选择为启用或不启用记录所有异常。
动作	当发现异常，将执行该动作。如果该行为设置为通过，将允许异常流量通过，否则阻断异常流量。
阀值	判定是否为异常的临界值。

DoS 传感器保护地址参数信息

参数名称	参数说明
目的地址	目的 IP 地址为 0.0.0.0/0 时为所有的地址。如果 ZXSEC US 设备以透明的模式运行，0.0.0.0/0 也包括管理 IP 地址。
目的端口	流量的目的端口，0 表示所有端口。
源地址	源 IP 地址为 0.0.0.0/0 时为所有的地址。
添加	在输入目的地址，目的端口和源地址后，在列表中添加保护地址。当符合三个地址条件后，会调用该传感器进行流量监测。如果没有设置地址，则该传感器检测所有流量。

25.7.3 了解异常

针对 TCP，UDP 和 ICMP 每个协议，DoS 传感器提供 4 个统计型异常检测，总共有 12 个可配置的异常检测。

12 个独立可配置异常参数信息

异常	描述
tcp_syn_flood	如果向一个目标 IP 地址的 SYN 发包率（包括重发）超过配置阀值，执行相应动作。阈值表示每秒钟的发包数量。
tcp_port_scan	如果从同一源端口的并发 TCP 连接数超过配置阀值，执行相应动作。阈值表示每秒钟的发包数量。
tcp_src_session	如果从同一个源 IP 地址的并发 TCP 会话数超过配置阀值，执行相应动作。
tcp_dst_session	如果到一个目标地址的并发 TCP 会话数超过配置的阀值，执行相应动作。
udp_flood	如果到一目标 IP 地址的 UDP 流量超过配置的阀值，执行

异常	描述
	相应动作。
udp_scan	如果由同一个源 IP 地址引发的 UDP 会话数超过配置阀值，执行相应动作。
udp_src_session	如果来自一源 IP 地址的并发 UDP 会话数超过配置阀值，执行相应动作。
udp_dst_session	如果连接到一目标 IP 地址的 UDP 会话数超过配置阀值，执行相应动作。
icmp_flood	如果发送到目标 IP 地址的 ICMP 包的数量超过配置阀值，执行相应动作。
icmp_sweep	如果由一源 IP 地址发起的 ICMP 包数量超过配置阀值，执行相应动作。
icmp_src_session	如果来自同一个源 IP 地址的并发 ICMP 连接数超过配置的阀值，执行相应动作。
icmp_dst_session	如果到一个目标 IP 地址的并发 ICMP 连接数超过配置阀值，执行相应动作。

25.8 IPS CLI 配置

这一部分描述通过 CLI 配置的 IPS 扩展功能。

ips global fail-open

当 IPS 功能出现问题不能正常工作时，ZXSEC US 设备默认其它功能模块继续工作，并且不会阻塞网络流量。

ips global socket-size

设置 IPS 的缓冲区大小。

第26章 Web 过滤

26.1 概述

描述

本章围绕四个部分，web 过滤功能、web 过滤内容屏蔽、URL 过滤与 US Service web 过滤，相互补充提供对互联网用户最大的控制与保护。

内容

26.2 Web 过滤的操作顺序

应用 web 过滤的具体操作顺序：

1. URL 免除（web 免除列表）
2. URL 屏蔽（Web URL 屏蔽）
3. URL 屏蔽（web 模式屏蔽）
4. US Service web 过滤（也称为分类屏蔽）
5. 内容屏蔽（web 内容屏蔽）
6. 脚本过滤（web 脚本过滤）
7. 反病毒扫描

URL 过滤列表是按以上的顺序执行操作的。（USOS v2.80 系统下，URL 过滤是无序执行的）。如果免除列表扫描中发现匹配，剩下的操作将不会继续进行。

本地分类查看要优先于 US Service web 过滤分类。

ZXSEC US 设备根据顺序允许以上的过滤程序，不符合其中的规则，网站将被自动屏蔽，不考虑之后的过滤操作设置。

26.3 Web 过滤是怎样生效的

以下的信息是阐述有关过滤操作之间如何应用生效，并就如何根据网络配置情况发挥各个操作的优势。

第一部分，URL 免除与屏蔽过滤将允许您对具体的地址采取怎样的动作。例如，您将配置 www.google.cn 免除被扫描，您可以将该网址添加到 URL 免除列表中，那么对该网站就不执行 web 过滤或病毒扫描的操作。

如果您已经设置屏蔽了一种文件模式，同时一些用户需要访问这些被屏蔽中的 URL，这时，您可以在 US Service web 过滤选项中配置跳过设置。也就是设置哪些用户可以访问被屏蔽的 URL，以及访问的时间长度。例如，您配置允许用户 1 能够访问 wwww.fakeLAND.com 一个小时。您可以设置建立一个豁免列表，列表中的任何使用跳过功能的用户在被允许访问屏蔽的 URL 之前必须填写在线的验证表格。

US Service web 过滤配置也允许您创建本地类别以屏蔽一些 URL 组。在您创建了类别后，您可以使用本地分类将一些具体的网站添加到您所创建的本地分类中。然后，您可以使用“防火墙>保护内容表”配置 US Service 对本地类别所采取的动作。本地分类过滤优先于 US Service 过滤。

最后，US Service 服务可以对 ActiveX，Cookie 与 Java applet 应用脚本过滤，进入“防火墙>保护内容表>web 过滤”中配置。

在您完成所有这些配置设置后，您还需要进入“防火墙>保护内容表>web 过滤”与“防火墙>保护内容表>US Service web 过滤”启动这些配置。

以下有关如何配置 web 过滤选项的说明。Web 过滤功能必须在激活的保护内容表中对应的设置后才生效。

26.4 Web 过滤

按照常规的步骤，您进入 web 过滤选项中配置 web 过滤设置并在保护内容表中启动所要使用的过滤项。进入“防火墙>保护内容表”激活启动的过滤配置。



注意：

启动意思是在您开启 web 过滤项时，过滤将被使用。启动并不是意味着过滤配置已经开始生效。使所有启动的过滤器生效，您必须进入“防火墙>保护内容表”。

有关 US Service-网页过滤的详细信息，将在第“US Service-网页过滤选项”中详细说明。对于新的网页的分类以及建议分类类型可以提交到 US Service 中心。有关链接到 US Service 中心的详细信息，参见中兴通讯公司网站知识库。

web 过滤以及内容保护列表 web 内容屏蔽配置

保护内容标 web 过滤选项	web 过滤>内容屏蔽
Web 内容屏蔽	Web 过滤>内容屏蔽
根据内容屏蔽列表中所列禁忌的词汇启动或撤消对于 HTTP 流量的网页屏蔽功能。	在内容屏蔽列表中添加词汇或模式，以屏蔽含有这些词汇与模式的网页。

web 过滤以及内容保护列表网址过滤

屏蔽网页 URL	web 过滤>URL 屏蔽
基于 URL 屏蔽列表启动或撤消对于 HTTP 网页内容过滤功能。	在 URL 屏蔽列表中添加具体的源 URL，以屏蔽这些 URL。

web 过滤以及内容保护列表中脚本以及下载文件过滤

内容保护表 web 过滤选项	web 过滤设置
动态 X 插件过滤，Cookie 过滤，JavaApplet 插件过滤。	n/a
启动或中止 HTTP 流量中网页的脚本过滤。	
Web 重续下载屏蔽	n/a
启动阻止已经下载了部分的文件。启动该功能选项可以防止无意中可能下载的是病毒文件，但是可以导致下载中断。	

web 过滤以及内容保护列表中 web 类型过滤配置

启动网页类型过滤	web 过滤>类型屏蔽>配置
启动 US Service web 过滤功能。（只适用于 HTTP 流量）	US Service web 过滤>配置
启动 US Service web 过滤豁免（只适用于 HTTP 流量）	US Service web 过滤>过滤豁免
提供被屏蔽的 4XX 以及 5XX 错误的详细信息。（只适用于 HTTP 流量）	
根据 URL 分类图像（被屏蔽的图像将以空白页替代）（只适用于 HTTP 流量） US Service web 过滤返回的分类错误网页时，允许该网页通过并显示。	
严格屏蔽（只适用于 HTTP 流量）	
类型/动作	
US Service web 过滤服务对各种网页进行总结分类从而过滤	

启动网页类型过滤	**web 过滤>类型屏蔽>配置**
为不同类型的网页。您可以设置对不同类型的网页采取不同的动作，如允许通过、屏蔽、日志记录或添加在豁免名单中。	
本地类型可以根据本地需要配置最合适的类型。	US Service web 过滤>本地类型|本地分类
类别/动作	
启动该选项后，用户可以访问那些提供内容缓存，以及提供搜索图像、音频以及视频文件功能的网站。并可以对不同类别的网站采取不同的动作，如允许通过、屏蔽、日志记录或添加在豁免名单中。	

访问内容保护表中的 **web** 过滤选项

1. 进入“防火墙>保护内容表”。
2. 点击编辑或新建。
3. 设置 web 过滤或 web 类别过滤。



注意：

如果 US 设备中启动了虚拟域，可以对 web 过滤功能进行全局配置。在主菜单项中点击“全局配置”可以访问 web 过滤或 web 类型过滤功能。

26.5 内容屏蔽

通过屏蔽具体的词或短语控制网页内容的显示。如果在内容保护列表中启动该功能，ZXSEC US 设备按照设定的禁忌词汇在所要求的网页中查找。如果在网页中发现与设定的禁忌词汇相匹配的词，将计算累加数量。如果数量超过用户定义的值，该网页将被屏蔽。

您可以使用 Perl 正则表达式或通配符将禁忌词语添加在列表中。



注意：

Perl 正则表达式模式查询要求垃圾邮件过滤选项中禁忌词汇大小写都要符合。

配置使禁忌词汇成为不敏感匹配，使用常规表达式/i.例如，/bad language/I

将屏蔽所有含有 bad language 的全部邮件。通配符模式不是大小写敏感的模式。

26.5.1 查看网页内容屏蔽列表目录

您可以在 ZXSEC US 设备的网页内容列表中添加多个网页内容屏蔽列表，并针对每项内容保护项选择最佳的网页内容屏蔽列表。进入 web 过滤>内容屏蔽，查看网页内容列表目录。点击目录中每个列表对应编辑图标可以编辑该列表。

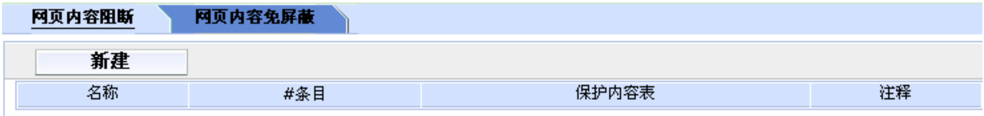


图26.5-1　网页内容屏蔽列表目录

网页内容屏蔽列表目录中的图标以及其功能：

参数信息

参数名称	参数说明
添加	在目录中添加新的列表，输入列表名称并点击添加。新建的列表在默认情况下是空的。
名称	网页内容屏蔽列表可用的名称。
#条目	每个网页内容屏蔽列表中内容模式的编号。
内容保护列表	每个网页内容屏蔽列表应用的内容保护列表。
描述	作为可选项，对每个网页内容屏蔽列表添加描述内容。描述内容限于 63 个字符长度。超过这个长度，便会被截去。空格键也将会被加号（+）取代。
删除图标	点击从目录中删除网页内容屏蔽列表。如果该列表应用于内容保护列表将不能被删除。
编辑图标	点击编辑网页内容屏蔽列表的列表名称以及描述信息项。

选择网页内容屏蔽列表添加在内容保护列表中。详细信息，参见“web 过滤选项”。

26.5.2 创建新的网页内容屏蔽列表

进入 web 过滤>内容屏蔽并点击“新建”在网页内容屏蔽列表目录中添加网页内容屏蔽列表。

新列表	
名称	
注释	(最大63个字符)
确定	取消

图26.5-2 新建网页内容屏蔽列表

参数信息

参数名称	参数说明
名称	输入新建列表的名称。
注释	如需要，输入对该列表描述性的内容。

26.5.3 查看网页内容屏蔽列表

启动网页内容屏蔽功能后，每个被请求的网页都将于内容屏蔽列表进行匹配。将网页中出现的每个模式的值相加，如果总值超过内容保护列表中设定的阀值，该网页将被屏蔽。如果一个模式在网页中出现多次，该模式的值只在列表中生效计值一次。

进入 web 过滤>内容屏蔽，查看网页内容屏蔽列表。

网页内容阻断 网页内容免屏蔽

新建

名称	#条目	保护内容表	注释

图26.5-3 网页内容屏蔽列表

注意：

请在防火墙保护内容表中在 web 过滤项下启动网页内容屏蔽激活内容屏蔽设置。

网页内容屏蔽列表的图标以及其功能：

参数信息

参数名称	参数说明
名称	网页内容屏蔽列表名称。在名称字段可以编辑修改名称信息。ZXSEC US1300 以及该型号以上的设备支持该功能。
注释	可选项。点击添加描述信息。ZXSEC US1300 以及该型号以上的设

参数名称	参数说明
	备支持该功能。
新建	点击“新建”在网页内容屏蔽列表中添加新的模式。
总数	网页内容屏蔽列表中包含模式条目的数量
翻上页图标	点击查看上一页。
翻下页图标	点击查看下一页。
删除条目图标	点击删除列表。
禁忌词汇	当前禁忌词汇列表。选中功能框启动列表中所有的项目。
样式	禁忌词汇与模式列表。选中该选项的功能框，启动显示列表中全部的禁忌词汇。
模式类型	禁忌词汇列表条目使用的模式类型。如常规表达式或通配符。参见“使用 Perl 正则表达式”。
语言	选择所要屏蔽的字符属于哪个语种：简体中文，繁体中文，法语，日本语，韩语，泰语或西文。
打分	应用于模式的权值。在网页中出现的相匹配的值相加，如果该值超出内容保护列表中设置的值，网页将被屏蔽。
删除图标	点击从列表中删除条目。
编辑图标	点击编辑以下信息：禁忌词汇、模式类型以及语言选项。

26.5.4 配置网页内容屏蔽列表

禁忌词汇可以设置为一个词或是一段最多 80 个字符长度文字字符串。列表中的禁忌词汇最多可以添加 9000 条。

进入 web 过滤>内容屏蔽，添加或编辑内容屏蔽模式。

新建屏蔽样式
样式
模式类型 通配符
语言 简体中文
Score 10
激活
OK 取消

图26.5-4 新建内容屏蔽模式列表

参数信息

参数名称	参数说明
样式	输入所要添加的禁忌词汇或模式。对于输入的单个词，ZXSEC US 设备将在所接收的所有网页中检索该词。对于输入的词组，ZXSEC US 设备将在所接收的所有网页中检索包含该词组中任何一个词。如果对该词组加上引号，ZXSEC US 设备将在接收的网页中检索与该词组完全相匹配的信息。
模式类型	禁忌词汇列表条目使用的模式类型。如常规表达式或通配符。参见“使用 Perl 正则表达式”。
语言	选择所要屏蔽的字符属于哪个语种：简体中文，繁体中文，法语，日本语，韩语，泰语或西文。
计值	输入出现该禁忌词汇的总计的数值。
激活	选中“激活”功能框激活列表中模式。

26.5.5 查看网页内容免屏蔽列表目录

您可以在 ZXSEC US 设备的网页内容列表中添加多个网页内容免除列表，并针对每项内容保护项选择最佳的网页内容免除列表。进入 web 过滤>内容屏蔽>网页内容免除列表，查看网页内容列表目录。点击目录中每个列表对应编辑图标可以编辑该列表。

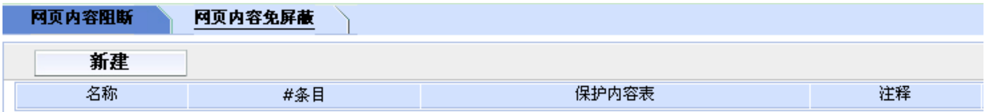


图26.5-5　网页内容免屏蔽列表目录

参数信息

参数名称	参数说明
新建	在目录中添加新的列表，输入列表名称并点击添加。新建的列表在默认情况下是空的。
名称	网页内容屏蔽列表可用的名称。
#条目	每个网页内容屏蔽列表中内容模式的编号。
内容保护列表	每个网页内容屏蔽列表应用的内容保护列表。
注释	作为可选项，对每个网页内容屏蔽列表添加描述内容。
删除图标	点击从目录中删除网页内容屏蔽列表。如果该列表应用于内容保护列表将不能被删除。
编辑图标	点击编辑网页内容屏蔽列表的列表名称以及描述信息项。

选择网页内容屏蔽列表添加在内容保护列表中。详细信息，参见“web 过滤选项”。

26.5.6 创建新的网页内容免屏蔽列表

进入 web 过滤>内容屏蔽>网页内容免屏蔽，并点击“新建”在网页内容免除列表目录中添加网页内容免除列表。

图26.5-6 新建网页内容免屏蔽列表

参数信息

参数名称	参数说明
名称	输入新建列表的名称。
注释	如需要，输入对该列表描述性的内容。

26.5.7 查看网页内容免屏蔽列表

网页内容免除列表是网页内容屏蔽功能的延伸。如果网页内容免除列表中定义的任何模式在网页中出现，该网页将不能被屏蔽，即使网页内容屏蔽功能应用应该将该网页屏蔽。

进入 web 过滤>内容屏蔽>网页内容免屏蔽，查看网页内容屏蔽列表。

图26.5-7 网页内容免屏蔽列表



注意：

在防火墙保护内容表中在 web 过滤项下启动网页内容屏蔽激活内容屏蔽设置。

网页内容免屏蔽列表各参数信息

参数名称	参数说明
名称	网页内容免除列表名称。在名称字段可以编辑修改名称信息。
注释	可选项。点击添加描述信息。ZXSEC US1300 以及该型号以上的设备支持该功能。
新建	点击“新建”在网页内容免除列表中添加新的模式。
总数	网页内容免除列表中包含模式条目的数量。
翻上页图标	点击查看上一页。
翻下页图标	点击查看下一页。
删除条目图标	点击删除列表。
样式	当前列表中的模式。选中功能框启动列表中所有的模式。
样式类型	免除词汇列表条目使用的模式类型。如常规表达式或通配符。参见“使用 Perl 正则表达式”。
语言	选择所要屏蔽的字符属于哪个语种：简体中文，繁体中文，法语，日本语，韩语，泰语或西文。
删除图标	点击从列表中删除条目。
编辑图标	点击编辑以下信息：禁忌词汇、模式类型以及语言选项。

26.5.8 配置网页内容免除列表

网页内容模式可以设置为一个词或是一段最多 80 个字符长度文字字符串。列表中的禁忌词汇最多可以添加 9000 条。

进入 web 过滤>内容免除，添加或编辑内容屏蔽模式。

新列表

名称

注释 (最大63个字符)

确定 取消

图26.5-8 新建内容免除模式列表

参数信息

参数名称	参数说明
样式	输入所要添加的内容免除模式。对于输入的单个词，ZXSEC US 设备将在所接收的所有网页中检索该词。对于输入的词组，ZXSEC US 设备将在所接收的所有网页中检索包含该词组中任何一个词。如果对该词组加上引号，ZXSEC US 设备将在接收的网页中检索与该词组完

参数名称	参数说明
	全相匹配的信息。
样式类型	禁忌词汇列表条目使用的模式类型。如常规表达式或通配符。参见“使用 Perl 正则表达式”。
语言	从下拉菜单中选择语言。
启动	选中“启动”功能框激活列表中模式。

26.6 网址 URL 过滤

您可以通过将具体的 URL 添加在 URL 列表中设置允许或屏蔽对这些 URL 的访问。使用文本格式或正则表达式（或通配符字符集）添加所要屏蔽 URL 的模式。ZXSEC US 设备屏蔽与任何指定的 URL 或模式相匹配的 URL 并显示以替换信息。



注意：

在防火墙保护内容表中在 web 过滤项下启动网页内容屏蔽激活内容屏蔽设置。URL 屏蔽功能并不妨碍用户使用网页浏览器对其它网络服务的访问。例如，URL 屏蔽功能并不阻止对 ftp://ftp.badsite.com 的访问，但是，您可以使用防火墙策略拒绝 FTP 连接。

26.6.1 查看网址过滤列表目录

您可以在 ZXSEC US1300 设备的网页内容列表中添加多个网址过滤列表，并针对每项内容保护项选择最佳的网址过滤列表。进入 web 过滤>网址过滤列表，查看网址过滤列表目录。点击目录中每个列表对应编辑图标可以编辑该列表。

网址过滤

新建

名称	#条目	保护内容表	注释

图26.6-1 网址过滤列表目录

网址过滤列表目录中参数信息

参数名称	参数说明
新建	在目录中添加新的列表，输入列表名称并点击添加。新建的列表在默认情况下是空的。
名称	网址过滤列表可用的名称。
#条目	每个 URL 列表中 URL 模式的编号。

参数名称	参数说明
保护内容表	每个网址过滤列表应用的内容保护列表。
描述	作为可选项，对每个网址过滤列表添加描述内容。
删除图标	点击从目录中删除网址过滤列表。如果该列表应用于内容保护列表将不能被删除。
编辑图标	点击编辑网页内容屏蔽列表的列表名称以及描述信息项。

选择网址过滤列表添加在内容保护列表中。详细信息，参见“web 过滤选项”。

26.6.2 创建新的网址过滤列表

进入 web 过滤>网址过滤列表并点击“新建”在网页内容屏蔽列表目录中添加网址过滤列表。

图26.6-2　新建网址过滤列表

参数信息

参数名称	参数说明
名称	输入新建列表的名称。
注释	如需要，输入对该列表描述性的内容。
查看网址过滤列表	您可以设置在 URL 屏蔽列表中添加指定的 URL 屏蔽或免除对其的屏蔽。在 URL 屏蔽列表中添加以下选项： ● 完整的 URL 地址 ● IP 地址 ● 部分 URL 屏蔽全部的子域名

进入 web 过滤>网址过滤，查看网址过滤列表。

图26.6-3　网址过滤列表

网页内容屏蔽列表的图标以及其功能：

参数信息

参数名称	参数说明
名称	网址过滤列表名称。在名称字段可以编辑修改名称信息。ZXSEC US1300 以及该型号以上的设备支持该功能。
描述	可选项。点击添加描述信息。
新建	点击“新建”在网址过滤列表中添加新的 URL。
翻上页图标	点击查看上一页。
翻下页图标	点击查看下一页。
删除条目图标	点击删除列表。
URL	当前屏蔽/免除的 URL 名单。选中功能框，启动列表中全部的 URL。
类型	网址过滤列表条目使用的模式类型。如简单或常规表达式。
动作	发现匹配的 URL 时采取的动作：允许、屏蔽或免除屏蔽。 ● 允许：出现匹配条目，继续其它 web 过滤操作。 ● 免除屏蔽：出现匹配条目后，停止所有其它后续检测，包括 AV 扫描。 ● 屏蔽：屏蔽出现的匹配条目，停止其它 web 过滤操作。
删除图标	点击从列表中删除条目。
编辑图标	点击编辑以下信息：URL、类型以及动作。
移动图标	点击该图标弹出“移动网址过滤项”对话框。

26.6.3 配置网址过滤列表

URL 列表中最多可以添加 9000 个条目。



注意：

您可以输入一些顶极域名的后缀（如“com”后缀）屏蔽所有含有该域名后缀的 URL。

进入 web 过滤>网址过滤名单，在列表中添加 URL。

新建网址过滤器

网址

类型 简单

操作 阻断

启动

OK 取消

图26.6-4　新建网址过滤名单

参数信息

参数名称	参数说明
URL	输入 URL。输入的 URL 不要包括 http://。
类型	从下拉菜单中选择类型：simple 或常规表达式。
动作	从下拉菜单中选择动作：允许、屏蔽或免除屏蔽。
启动	选中该功能框启动 URL 列表。

输入顶级的 URL 或 IP 地址限制对该网站中所有网页的访问。例如，输入 www.example.com 或 192.168.144.155 将屏蔽对该网站中所有网页的访问。

输入顶级 URL 并在其后添加路径以及文件名，控制对该网站中某个网页的访问。例如，输入 www.example.com/news.html 或 192.168.144.155/news.html 将屏蔽对该网站中这个网页的访问。

将 example.com 添加到过滤列表中，限制对所有以 example.com 结尾的 URL 的访问。例如，将 example.com 添加到过滤列表中，将屏蔽对 www.example.com，mail.example.com，www.finance.example.com 等以 example.com 结尾的网页的访问。

使用文本格式或常规表达式建立一些 URL 的表达式可以屏蔽所有与该表达式相匹配的 URL。例如，example.*将于 example.com，example.org，example.net 等网页或网站相匹配。

ZXSEC US 设备的 web 模式屏蔽功能支持常规表达式。

注意：

对 URL 模式项设置动作为免除屏蔽的项目将不接受病毒扫描。如果网络中用户通过 ZXSEC US 设备从信任网站中下载文件，如果该网站的 URL 是添加在网址过滤列表中并且动作设置为免除屏蔽，那么 ZXSEC US 设备将对从该网站下载的文件不进行常规的病毒扫描。请在防火墙保护内容表中在 web 过滤项下启动网页内容屏蔽激活网址过滤设置。

26.6.4 在网址过滤列表中移动 URL 项

为了方便网址过滤列表的使用，网址过滤项可以在列表中移动不同的位置。打开网址过滤列表，点击所要移动过滤项对应的移动图标。

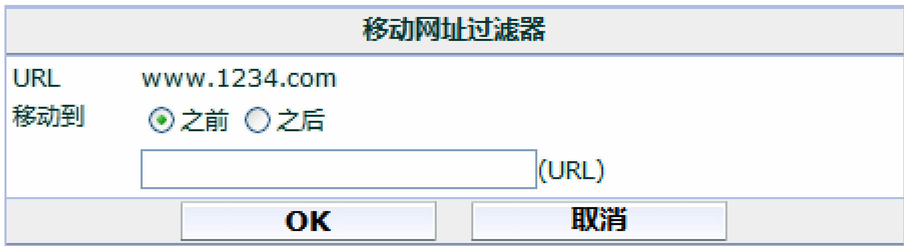


图26.6-5 移动网址过滤项

参数信息

参数名称	参数说明
移至	选择将 URL 项移动到列表中的新的位置。(URL)
设置	将过滤项移动到输入这项的之前或之后.

26.7 US Service-网页（web）过滤

US Service-网页服务是中兴通讯公司推出的可管理性的网页过滤服务解决方案。US Service-网页过滤服务将数百万的网页分为设定的一些类型范围，用户可以对过滤不同分类的网页采取允许通过，屏蔽以及监控的动作。ZXSEC US 设备将就近访问 US Serviceweb 过滤服务站点识别网页的类型然后执行用户或接口配置的防火墙策略。

US Service-网页过滤数据库包括超过 6 千万人工分类的网页。网页将被分为 56 个类型，用户可以对不同类型的网页实行允许通过，屏蔽或监控动作。随着互联网的不断发展，网页类型将不断的进行更新。用户可以配置将不同类型的网页分组

配置执行允许通过，屏蔽或监控动作，简化了配置。被屏蔽的网页将以信息页面替换说明根据互联网使用策略该网页不可达。

US Service 网页类型过滤是不同属性与方法结合对网页进行分类，包括分析网页正文，利用 web 结构以及人工分类。用户可以向 US Serviceweb 过滤服务站点对已分类网页类型的正确性提出置疑，根据用户的观点与意见，分类新的网址。

使用“配置网页类型选项”中所述操作步骤在保护内容表中配置 US Service-网页过滤类型。参见“配置 ZXSEC US 设备连接到 US SERVICE 中心并接收 US Service 服务”。

26.7.1 配置 US Service-网页过滤服务

进入系统管理>维护>US Service 中心，配置 web 过滤服务。其它配置信息，参见“配置 ZXSEC US 设备与 US SERVICE 中心连接以及接收 US Service 服务”。

26.7.2 查看优先（跳过）列表

用户可能需要访问那些被防火墙策略屏蔽的网站。这种情况下，管理员可以给用户设定一定的时间范围内对这些被屏蔽网站访问的权限。

当用户试图访问并屏蔽的网站，如果启动了优先设置，那么到该屏蔽网页访问链接将直接通往一个用户认证的页面。用户需要输入正确的用户名以及密码或是被屏蔽的网站名称。认证是基于用户组的，可以对本地、RADIUS 以及 LDAP 用户执行验证。有关认证以及配置用户组的详细信息，参见“用户组”。

进入 web 过滤>US Service-网页过滤服务>优先列表，查看优先列表信息。

跳过 本地类别 本地分类

名称	
管理跳过	
用户跳过	

图26.7-1 跳过列表

列表参数信息

参数名称	参数说明
新建	点击在列表中添加信息的优先规则。并显示该列表中的项目总数
翻上页	点击查看列表上一页信息。
翻下页	点击查看列表下一页信息。
清除全部图标	点击清除列表。

参数名称	参数说明
网址/类型	该项目是以 url 格式或是应用的类型所显示。
范围	访问该列表的用户或用户组范围。
离线网址	是否允许用户访问脱机状态下的 URL。绿色指示框表示允许脱机访问，灰色表示拒绝脱机访问。
创建人	优先规则的创建人。
结束日期	优先规则过期的时间。
删除图标	点击从列表中删除条目。
编辑图标	点击编辑以下信息：类型、URL、范围、用户、离线网址以及优先时间段。

26.7.3 配置优先规则

根据地址目录、域名或类型可以配置访问被屏蔽的网站。进入 web 过滤>US Service-网页过滤>跳过，创建跳过规则。

新建跳过规则

类型 目录

网址

范围 用户

用户

离线网址 允许

小时 17 分钟 18 秒 24

年 2008 月 Jun 日 4

确定 取消

图26.7-2 新建优先规则-地址或域名

参数信息

参数名称	参数说明
类型	选择地址或域名。
URL	输入网站的 URL 或域名。
范围	选择以下选项：用户、用户组、IP 或保护内容列表。根据所选的选项，在范围项中出现不同的功能设置项。
用户	在所选的范围选项内输入用户名称。

参数名称	参数说明
用户组	从下拉菜单中选择用户组。用户组必须在 US Service-web 配置之前设置。有关用户组的信息，参见“用户组”。
IP	输入创建优先规则用户的 IP 地址。
内容保护列表	从下拉菜单中选择内容保护列表项。
脱机 URL	该选项定义从屏蔽的 URL 中跳过的页面是否现显示图片或其它内容。 例如，所有的 US Service 类别都被屏蔽了，且您想访问的一个网站的图片可以有其它不同的域名提供。这时，您可以创建目录文件跳过该网站查看其中的网页。如果脱机访问功能被设置为拒绝，网页中所有的图片呈现不完整的显示，因为这些图片不是从您设置的跳过规则的网站申请的。如果脱机功能设置为允许，图片将正常显示。只有那些在页面跳过范围内设置跳过规则的用户可以从暂时性的跳过允许下查看这些图片。
优先期限	设置优先期限的时间。在优先列表中显示时便开始计算过期期限。

进入 web 过滤>US Service-网页过滤>跳过列表，创建优先列表的类型。

新建跳过规则

类型 类别

类别

类别	跳过
潜在不良后果的 (12)	☐
引起反感的或有争议的 (14)	☐
潜在消极因素的 (9)	☐
潜在浪费带宽 (5)	☐
潜在不安全的 (2)	☐
大众兴趣 (24)	☐
商业导向 (5)	☐
其他 (5)	☐
不在分类中	☐
本地类别 (0)	☐

分级

分级	跳过
缓冲中的内容	☐
搜索多媒体	☐
搜索图片	☐
搜索音频	☐
搜索视频	☐
垃圾邮件URL	☐

图26.7-3 新建跳过规则-类别

参数信息

参数名称	参数说明
类型	选择类别。
类别	选择优先项适用的类别。选择类别以及子类别。本地类别也将显示。分类 选择优先项应用的分类。设置了该功能项后，用户可以访问提供缓存以及提供图表、音频以及视频文件搜索的网站。
范围	选择以下选项：用户、用户组、IP 或保护内容列表。根据所选的选项，在范围项中出现不同的功能设置项。
用户	在所选的范围选项内输入用户名称。
用户组	从下拉菜单中选择用户组。用户组必须在 US Service-web 配置之前设置。有关用户组的信息，参见“用户组”。
IP	输入创建优先规则用户的 IP 地址。
内容保护列表	从下拉菜单中选择内容保护列表项。
离线网址	设置允许或屏蔽动作。该设置允许访问网站的链接。

参数名称	参数说明
持续时间	设置优先期限的时间。在优先列表中显示时便开始计算过期期限。

26.7.4 创建本地 URL 类型

可以创建用户定义的类别，设置允许用户在每项内容保护项的基础上屏蔽 URL 组。当配置内容保护列表时在这里定义的本地 URL 都将在整体 URL 类别列表中显示。用户可以根据本地的类型对 URL 进行分类。

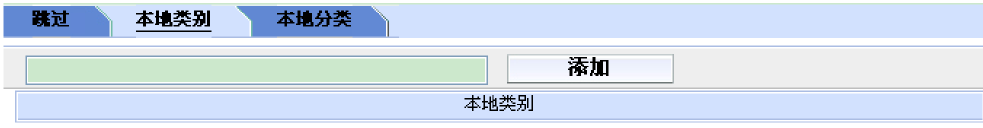


图26.7-4　本地类别列表

参数信息

参数名称	参数说明
添加	输入类别的名称，点击添加。
删除图标	从列表中删除条目。

26.7.5 查看本地分类列表

进入 web 过滤>US Service-网页过滤>本地分类，查看本地分类列表。



图26.7-5　本地分类列表

参数信息

参数名称	参数说明
新建	点击在列表中添加新的分类项。
查找	输入过滤列表的查找规则。1 到 n/n 列表中本地分类的总数。
翻上页图标	点击查看上一页信息。
翻下页图标	点击查看下一页信息。
清除全部图标	点击清除列表。
网址	分类的网址。
类别	URL 应用的类别或分类类型。如果 URL 被分类为不同的类型或分类时，需要用逗点分隔。点击灰色的漏斗形图标可以打开类型过滤对话框。当列表已经进行过滤后，漏斗图标呈绿色显示。

参数名称	参数说明
删除图标	点击删除列表中的条目。
编辑图标	点击编辑以下信息：URL、类别、分类项目。

新建本地类别判定

网址

类别判定

类别	判定
潜在不良后果的（12）	☐
引起反感的或有争议的（14）	☐
潜在消极因素的（9）	☐
潜在浪费带宽（5）	☐
潜在不安全的（2）	☐
大众兴趣（24）	☐
商业导向（5）	☐
其他（5）	☐
不在分类中	☐
本地类别（0）	☐

级别判定

分级	判定
缓冲中的内容	☐
搜索多媒体	☐
搜索图片	☐
搜索音频	☐
搜索视频	☐
垃圾邮件URL	☐

图26.7-6　类别过滤

参数信息

参数名称	参数说明
清除过滤项	点击清除过滤项.
类别名称	点击蓝色三角箭头扩展类别项。
启动过滤器	选中过滤项功能框启动过滤功能。
分级名称	能够被过滤的分类项名称。
启动过滤器	选中过滤项功能框启动过滤功能。

26.7.6 配置本地过滤

可以创建用户定义的类别，设置允许用户在每项内容保护项的基础上屏蔽 URL 组。对本地 URL 的分类将被包括在整体的网址列表中。

用户可以设定是否本地 URL 分类与 US Service 分类服务同时使用，或者本地分类优先于 US Service 分类服务。

进入 web 过滤>US Service-网页过滤>本地分类，创建本地分类。

新建本地类别判定

网址

类别判定

类别	判定
潜在不良后果的（12）	☐
引起反感的或有争议的（14）	☐
潜在消极因素的（9）	☐
潜在浪费带宽（5）	☐
潜在不安全的（2）	☐
大众兴趣（24）	☐
商业导向（5）	☐
其他（5）	☐
不在分类中	☐
本地类别（0）	☐

级别判定

分级	判定
缓冲中的内容	☐
搜索多媒体	☐
搜索图片	☐
搜索音频	☐
搜索视频	☐
垃圾邮件URL	☐

图26.7-7　新建本地分类

参数信息

参数名称	参数说明
网址	输入需要分类的网址。
类型名称	点击蓝色箭头扩展类型项。
判定	选中过滤项功能框启动过滤功能。

参数名称	参数说明
分级	输入需要分类的类别项。
判定	启动分类过滤。

26.7.7 类型屏蔽的 CLI 配置

如果需要更改默认的 US Service 网页过滤服务站点的主机名称，使用 webfilter US Service 命令的关键字 hostname。使用基于 web 的管理器不能够更改 US Service-web 服务站点的主机名称。您可以使用 CLI 配置全部的 US Service 网页过滤服务的设置。参见 ZXSEC US 设备 CLI 使用参考手册有关 webfilter US Service 命令全部的关键字说明。

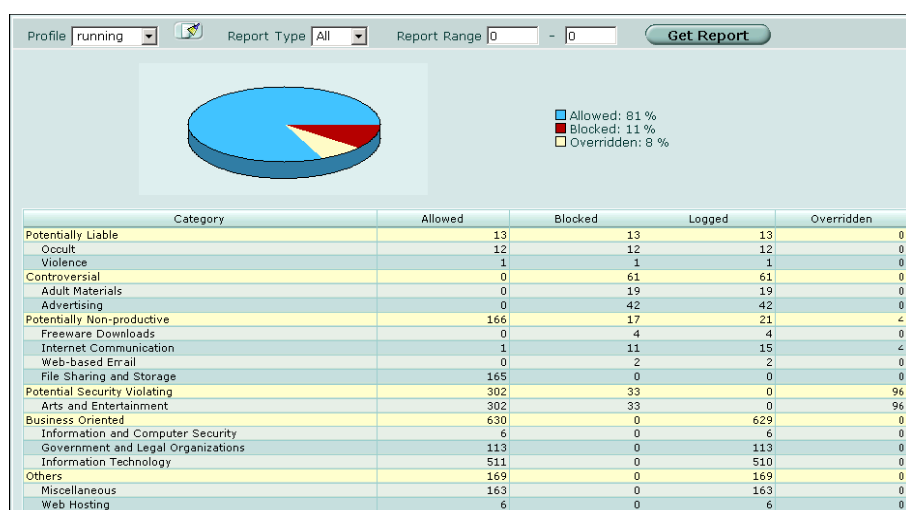
26.7.8 US Service-网页过滤功能报告



注意：

只有配置了本地硬盘的 ZXSEC US 设备可以查看 US Service-网页过滤报告。您可以配置 ZXSEC US 设备对任何的保护内容表中 web 过滤操作生成文本格式或饼状图格式的报告。ZXSEC US 设备保持对每一类型 web 过滤设置允许、屏蔽或监控的网页数量记录。您可以设置查看一定时间范围内的报告，或查看全部活动的报告。

进入 web 过滤>US Service-网页过滤>报告，创建 web 过滤报告。



Category	Allowed	Blocked	Logged	Overridden
Potentially Liable	13	13	13	0
Occult	12	12	12	0
Violence	1	1	1	0
Controversial	0	61	61	0
Adult Materials	0	19	19	0
Advertising	0	42	42	0
Potentially Non-productive	166	17	21	4
Freeware Downloads	0	4	4	0
Internet Communication	1	11	15	4
Web-based Email	0	2	2	0
File Sharing and Storage	165	0	0	0
Potential Security Violating	302	33	0	96
Arts and Entertainment	302	33	0	96
Business Oriented	630	0	629	0
Information and Computer Security	6	0	6	0
Government and Legal Organizations	113	0	113	0
Information Technology	511	0	510	0
Others	169	0	169	0
Miscellaneous	163	0	163	0
Web Hosting	6	0	6	0

图26.7-8　US Service-网页过滤报告

以下生成报告的选项：

参数信息

参数名称	参数说明
内容保护列表项	选择所要生成报告的内容保护列表项。
报告类型	设置生成报告的时间范围。设置时间范围的选项为：小时，天，或所有历史记录。
报告范围	设置报告生成的小时范围（24 小时制）或以天计（六天之前到至今）。例如，您设置报告生成的类型为小时制并输入为 13 到 16，那么所生成的是下午 1 点到 4 点之间屏蔽报告。如果您设置报告生成的类型为以天计算并在范围中键入 0 到 3，那么所生成的是三天前到今天的屏蔽报告。
生成报告	点击“生成报告“。

生成的报告包含以下信息：

- 类型：生成数据报告的类型。
- 通过：在设置的时间范围内允许通过的网页比列。
- 屏蔽：在设置的时间范围内屏蔽的网页比列。
- 监控：在设置的时间范围内配置监控的网页所占的比列。

第27章 反垃圾邮件

27.1 概述

描述

本章是有关如何配置内容保护列表项中垃圾邮件过滤功能。

内容

27.2 垃圾邮件过滤

垃圾邮件过滤功能是通过检测垃圾邮件，识别已知或可疑的垃圾邮件发送服务器发送邮件来管理未经请求发送的商业性邮件。对系统应用模块进行的广泛的垃圾邮件过滤服务同时，您可以根据每项配置文件的基础上启动垃圾邮件过滤。

US Service 反垃圾服务是中兴通讯公司提供的反垃圾邮件系统，该系统包括一个 IP 地址黑名单，URL 黑名单与垃圾过滤选项工具。US Service 中心接受垃圾邮件信息的提交以及垃圾邮件误报信息的提交。详细信息，参见中兴通讯网站中知识库版块以及链接到 US Service 中心。

27.2.1 垃圾邮件过滤操作顺序

邮件传输的协议决定了向内邮件通过垃圾邮件过滤功能的顺序。

以 SMTP 协议传输的邮件

1. IP 地址 BWL 检索－最终中继 IP。
2. RBL&ORDBL 检索，IP 地址 USShield 检索，HELO DNS 查询。
3. 电子邮件地址 BWL 检索（从接收的邮件的标头中摘取 IP 地址，以及在邮件内容中摘取 URL）。
4. MIME 标头检索。

5. IP 地址 BWL 检索（从接收的标头中摘取的 IP 地址）。
6. 退回邮件 DNS 检索，US Service 反垃圾邮件检索，DNSBL & ORDBL。
7. 禁忌词汇检索。

以 POP3 与 IMAP 协议传输的邮件

1. MIME 标头检索，电子邮件地址 BWL 检索。
2. 对邮件主题进行禁忌词汇检索。
3. IP BWL 检索。
4. 对邮件主体进行禁忌词汇检索。
5. 退回地址邮件 DNS 检索，US Service 反垃圾邮件检索，RBL&ORDBL 检索

以 SMTP，POP3 以及 IMAP 协议传输的邮件

过滤选项需要从服务器查询请求并同时获得回复（US Service 反垃圾邮件服务与 DNSBL/ORBDL）。为了避免延迟，请求发送的同时运行另一项过滤项目。一经接收到回复，第一个触发的垃圾邮件采取的动作的回复将立即生效。

如果在一项过滤选项中没有出现匹配内容或发现问题，将立即轮下去执行下一项过滤项目。如果一个过滤项对所过滤的邮件采取了标注为垃圾邮件的动作，ZXSEC US 设备将根据保护设置文件中的设置对该邮件进行标识或丢弃（该动作只适用于 SMTP 邮件）。如果过滤选项将过滤的邮件采取了标注为干净邮件的动作，其它过滤项将直接放行该邮件。如果过滤项对邮件采取了标注为拒绝的动作，该邮件会话将被丢弃。被拒绝的 SMTP 邮件信息将以配置的替换信息替换。

垃圾邮件过滤是系统范围内的配置，但需要基于每项保护内容进行启动。

垃圾邮件过滤以及保护配置垃圾邮件过滤设置

保护内容表中垃圾邮件过滤选项	垃圾邮件过滤设置
IP 地址 US Service 反垃圾邮件服务检索	**系统管理>维护>US Service 服务中心**
启动或取消中兴通讯公司提供的反垃圾邮件服务称为 US Service 反垃圾邮件服务。US Service 反垃圾邮件服务是中兴通讯公司自有的 DNSBL，提供垃圾邮件发送 IP 地址与 URL 的黑名单。一旦发现新的垃圾邮件发送源，中兴通讯公司将及时更新该 DNSBL。	启动 US Service-反垃圾邮件，检索 US Service 反垃圾邮件服务服务器的状态，查看许可证类型以及许可证过期的时间并配置缓冲存储器。参见“配置 US 设备连接到 US SERVICE 中心以及 US Service 服务”

<table>
<tr><th>保护内容表中垃圾邮件过滤选项</th><th>垃圾邮件过滤设置</th></tr>
<tr><td>IP 地址 BWL 检索</td><td>垃圾邮件过滤>黑/白名单>IP 地址</td></tr>
<tr><td>黑白名单检索。启动或撤消将向内的 IP 地址与配置的垃圾邮件过滤IP地址列表检索。（只适用于以 SMTP 传输的邮件）。</td><td>您可以配置对识别为垃圾邮件的邮件所采取的动作，如清除或拒绝该 IP 地址发送的邮件。您可以将该 IP 地址放置在列表中的任何位置。垃圾邮件过滤检索将按顺检索每个 IP 地址。（只适用于以 SMTP 传输的邮件）。</td></tr>
<tr><td>DNSBL&ORDBL 检索</td><td>只能通过 CLI 命令配置</td></tr>
<tr><td>启动或中止将电子邮件流量在配置的 DNSBL 名单以及 ORDBL 名单服务器中进行检索。</td><td>从列表中添加或删除 DNSBL 以及 ORDBL 服务器。您可以设置对每台服务器识别为垃圾邮件的信息采取标注或拒绝该邮件的动作。（只适用于以 SMTP 传输的邮件）DNSBL 以及 ORDBL 服务器只有通过 CLI 命令配置。</td></tr>
<tr><td colspan="2">HELO DNS 查询</td></tr>
<tr><td colspan="2">启动或撤消在域名服务器中检测源域名。如果源域名与标注为垃圾邮件的 IP 地址不匹配，可以在配置文件中选择所要采取的动作。</td></tr>
<tr><td>电子邮件地址 BWL 检索</td><td>垃圾邮件过滤>黑/白名单>电子邮件地址</td></tr>
<tr><td>启动或撤消在配置的垃圾邮件过滤的邮件地址列表中检索向内的邮件地址。</td><td>使用通配符与常规表达式在列表中添加或编辑邮件地址。您可以配置对识别为垃圾邮件的邮件所采取的动作，如清除或拒绝该邮件地址发送的邮件。您可以将该邮件地址放置在列表中的任何位置。垃圾邮件过滤检索将按顺检索每个邮件地址。</td></tr>
<tr><td colspan="2">退回的电子邮件 DNS 检索</td></tr>
<tr><td colspan="2">启动或撤消将向内的邮件退回地址域名与域名服务器中配置的 IP 地址相匹配。如果退回地址域名与 IP 地址不匹配，该邮件将标注为垃圾邮件，您可以从保护配置中选择对该邮件采取的动作。</td></tr>
<tr><td>MIME 标头检索</td><td>通过 CLI 命令配置</td></tr>
<tr><td>启动或撤消在配置的垃圾邮件过滤 MIME 标头列表中检索 MIME 标头。</td><td>使用通配符与常规表达式在列表中添加或编辑 MIME 标头。您可以配置对识别为垃圾邮件的邮件所采取的动作，或清除包含该 MIME 标头的邮件。DNSBL 以及 ORDBL 服务器只有通过 CLI 命令配置。</td></tr>
<tr><td>禁忌词汇检索</td><td>垃圾邮件过滤>禁忌词汇</td></tr>
<tr><td>启动或撤消在配置的垃圾邮件过滤被禁词语列表中检索源邮件。</td><td>使用通配符与常规表达式在列表中添加与编辑被禁词语。您可以配置禁止的词语，或在邮件主题及正文中搜索该词汇。您也可以配置对识别为垃圾邮件的邮件所采取的动作或清除邮件中含有的被禁止词语。</td></tr>
<tr><td colspan="2">对垃圾邮件所采取的动作</td></tr>
<tr><td colspan="2">对识别为垃圾邮件的邮件所采取的动作。对以 POP3 或 IMAP 邮件采取标注为垃圾邮件的</td></tr>
</table>

保护内容表中垃圾邮件过滤选项	垃圾邮件过滤设置
动作。对 SMTP 邮件采取标注为垃圾邮件或丢弃该邮件的动作。您可以在被标注邮件的主题或 MIME 标头中附加评论。您也可以把对垃圾邮件所采取的动作记录在事件日志中。	
标注	
您可以在垃圾邮件的标注中输入词或短语。最多可以输入 63 个字符。	
附录	
输入词或短语附在被识别为垃圾邮件的邮件上。最多可以输入 63 个字符。	
在系统日志中添加事件信息	
启动或撤消将对垃圾邮件所采取的动作信息记录到日志事件中。	

进入防火墙>内容保护列表，访问垃圾邮件过滤选项，对垃圾邮件过滤功能进行编辑或创建。



注意：

如果 ZXSEC US 设备启动了虚拟域设置，垃圾邮件过滤功能可以进行全局配置。在主菜单项中点击全局配置，设置该功能项。

27.3 禁忌词汇

通过屏蔽含有具体的词汇或模式定义并识别为垃圾邮件。ZXSEC US 设备在邮件信息中搜索禁忌词汇。如果发现匹配选项，对该词语设置的值将累计相加。如果累加值超过用户所设置的阀值，该信息将被标注为垃圾邮件。如果没有发现相应的匹配，邮件将继续被发送继续执行下一个过滤项。

您可以使用 Perl 正则表达式或通配符将禁忌词汇模式添加在匹配查询列表中。参见“使用 Perl 正则表达式”。



注意：

Perl 正则表达式模式查询要求垃圾邮件过滤选项中禁忌词汇大小写都要符合。配置使禁忌词汇成为不敏感匹配，使用常规表达式/i.例如，/bad language/I 将屏蔽所有含有 bad language 的全部邮件。通配符模式不是大小写敏感的模式。

27.3.1 查看垃圾邮件过滤禁忌词汇列表目录

您可以在 ZXSEC US 设备的反垃圾邮件过滤的禁忌词汇列表中添加多个禁忌词汇，并针对每项内容保护项选择最佳的禁忌词汇列表。进入反垃圾邮件>禁忌词汇，

查看垃圾邮件过滤禁忌词汇列表目录。点击目录中每个列表对应编辑图标可以编辑该列表。

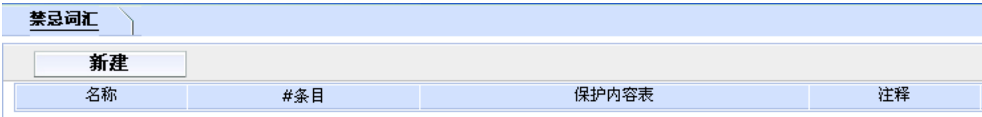


图27.3-1 反垃圾邮件禁忌词汇列表目录

参数信息

参数名称	参数说明
添加	在目录中添加新的列表，输入列表名称并点击添加。新建的列表在默认情况下是空的。
名称	垃圾邮件过滤禁忌词汇列表可用的名称。
#条目	列表中每个项目的编号。
内容保护表	每个禁忌词汇列表应用的内容保护列表。
注释	作为可选项，对每个禁忌词汇列表添加描述内容。
删除图标	点击从目录中删除禁忌词汇列表。如果该列表应用于内容保护列表将不能被删除。
编辑图标	点击编辑网页内容屏蔽列表的列表名称以及描述信息项。

选择禁忌词汇列表添加在内容保护列表中。详细信息，参见“垃圾邮件过滤选项”。

27.3.2 创建新的禁忌词汇列表

进入反垃圾邮件>禁忌词汇列表并点击“新建”在反垃圾邮件禁忌词汇列表目录中添加禁忌词汇列表。



图27.3-2 新建禁忌词汇列表

参数信息

参数名称	参数说明
名称	输入新建列表的名称。

参数名称	参数说明
注释	如需要，输入对该列表描述性的内容。

27.3.3 查看禁忌词汇列表

启动反垃圾邮件功能后，每个电子邮件信息都将与反垃圾邮件禁忌词汇列表进行匹配。将邮件主题或正文，以及在这二者中出现的每条禁忌的值相加，如果总值超过内容保护列表中设定的阀值，将根据内容保护列表中设定的对垃圾邮件采取的动作来处理该邮件。如果一条禁忌词汇在邮件信息中出现多次，该模式的值只在列表中生效计值一次。

进入反垃圾邮件>禁忌词汇，查看禁忌词汇列表。

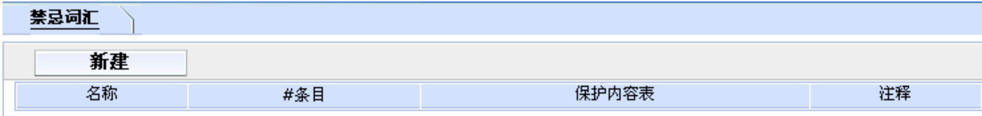


图27.3-3　禁忌词汇列表

参数信息

参数名称	参数说明
名称	禁忌词汇列表名称。在名称字段输入输入新的名称，点击 ok 确认可以生成新的列表名称。
注释	可选项。在描述字段中添加或编辑描述性信息。只有 ZXSEC US1300 或该型号以上的设备支持该功能。
新建	在禁忌词汇列表中添加新的禁忌词语以及词组。
全部	列表中条目的数量。
翻上页图标	点击查看上一页信息。
翻下页图标	点击查看下一页信息。
清除全部	点击清除全部列表信息。
模式	禁忌词汇的列表。选中“模式”功能框，启动在列表中显示全部禁忌词汇。
匹配类型	禁忌此类列表条目使用的模式类型。通配符或常规表达式。参见“使用 Perl 正则表达式”。
语言	选择所要屏蔽的字符属于哪个语种：简体中文，繁体中文，法语，日本语，韩语，泰语或西文。
作用范围	ZXSEC US 设备对邮件的主题，正文或两者都要查询是否含有列表中的禁忌词汇。
评分	应用于每条禁忌词汇的权值。在邮件信息中出现的所有的禁忌词汇的权值相加，如果总值超过内容保护列表中设置的 spamwordthreshold

参数名称	参数说明
	的值，根据该邮件使用的传输协议类型（例如对以 smtp3 传输的邮件所采取的处理动作）采取“通过”或“标注为垃圾邮件”这样的处理动作。如果一条词汇在邮件信息中出现多次，其值只在累加过程中生效一次。
删除图标	点击从列表中删除禁忌词汇。
编辑图标	点击编辑“模式”“匹配类型”“语言”“位置”与“动作”项。

27.3.4 配置反垃圾邮件禁忌词汇列表

禁忌词汇可以是一个单词或最多容纳 127 个字符的语句。如果您输入的是一个词，ZXSEC US 设备将屏蔽包含改词的所有邮件。如果您输入的是一个短语，ZXSEC US 设备将屏蔽包含与改短语精确匹配的邮件。屏蔽词句中含有的任何一个词，使用 Perl 正则表达式。参见“使用 Perl 正则表达式”。

进入反垃圾邮件>禁忌词汇，添加或编辑禁忌词汇。

图27.3-4 添加禁忌词汇

参数信息

参数名称	参数说明
模式	输入您所有添加在禁忌词汇列表中的词或词组。
匹配类型	禁忌此类列表条目使用的匹配类型。通配符或常规表达式。参见“使用 Perl 正则表达式”。
语言	选择所要屏蔽的字符属于哪个语种：简体中文，繁体中文，法语，日本语，韩语，泰语或西文。
作用范围	ZXSEC US 设备对邮件的主题，正文或两者都要查询是否含有列表中的禁忌词汇。
状态	选中该功能框，对邮件实行禁忌词汇查找扫描。

27.4 黑/白名单

启动了内容保护列表后，ZXSEC US 设备使用 IP 地址列表与邮件地址列表过滤向内的邮件。

在执行 IP 地址列表检索时，ZXSEC US 设备将发件人的 IP 地址在列表中按顺查找匹配。发现匹配后，将采取对应的保护设置动作。如果没有发现匹配选项，邮件将继续过滤到下一个过滤项。

ZXSEC US 设备将邮件发送人的邮件地址或域名与列表中的条目逐个匹配。如果发现匹配选项，对应的保护设置文件将对邮件采取动作。如果发现匹配，该邮件将被过滤到下一项垃圾邮件过滤选项。

查看反垃圾邮件 IP 地址列表您可以在 ZXSEC US 的设备反垃圾邮件选项中的黑/白名单中添加多个 IP 地址列表

并针对每项内容保护项选择最佳的 IP 地址列表。进入垃圾邮件过滤>黑/白名单>IP 地址，查看 IP 地址列表目录。点击目录中每个列表对应编辑图标可以编辑该列表。

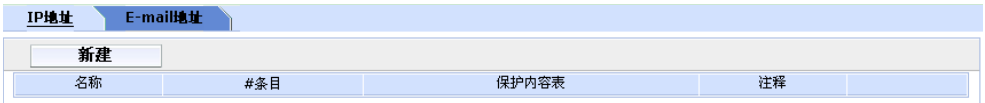


图27.4-1 反垃圾邮件 IP 地址列表目录

参数信息

参数名称	参数说明
添加	在目录中添加新的列表，输入列表名称并点击添加。新建的列表在默认情况下是空的。
名称	IP 地址列表可用的名称。
#条目	列表中每个项目的编号。
内容保护表	每个 IP 地址列表应用的内容保护列表。
注释	作为可选项，对每个 IP 地址列表添加描述内容。
删除图标	点击从目录中删除 IP 地址列表。如果该列表应用于内容保护列表将不能被删除。
编辑图标	点击编辑 IP 地址列表的“列表名称”以及“描述”项。

选择 IP 地址列表添加在内容保护列表中。详细信息，参见“垃圾邮件过滤选项”。

27.4.1 创建新的 IP 地址列表

进入反垃圾邮件>黑/白名单并点击“新建”在反垃圾邮件地址列表目录中添加邮件地址列表。

新列表
名称
注释 (最大63个字符)
确定 取消

图27.4-2 新建 IP 地址列表

参数信息

参数名称	参数说明
名称	输入新建列表的名称。
注释	如需要，输入对该列表描述性的内容。

27.4.2 查看 IP 地址列表

配置 ZXSEC US 设备从具体的 IP 地址中过滤邮件。ZXSEC US 设备将发件人的 IP 地址与系统中的列表进行逐个匹配。将每个 IP 地址标注为“干净”“垃圾邮件”或“拒绝”。您可以通过配置一个地址或掩码过滤单个的 IP 地址或地址范围。

进入反垃圾邮件>黑/白名单>IP 地址，查看 IP 地址列表。

IP地址 E-mail地址
新建
名称 #条目 保护内容表 注释

图27.4-3 IP 地址列表

参数信息

参数名称	参数说明
名称	IP 地址列表名称。在名称字段输入输入新的名称，点击 ok 确认可以生成新的列表名称。
注释	可选项。在描述字段中添加或编辑描述性信息。只有 ZXSEC US1300 或该型号以上的设备支持该功能。
新建	在 IP 地址列表中添加新的地址。
全部	列表中条目的数量。
翻上页图标	点击查看上一页信息。
翻下页图标	点击查看下一页信息。
清除全部	点击清除全部列表信息。
邮件地址	当前列表的 IP 地址。

参数名称	参数说明
动作	对与地址列表匹配的地址所采取的动作；标注为垃圾邮件，实行保护内容表中对垃圾邮件的处理方法；标注为干净邮件，允许该邮件通过下一过滤项；或标注为拒绝（只适用于 SMTP），丢弃会话。如果一个 IP 地址为标注为拒绝，但是是以 POP3 或 IMAP 传输的，该邮件将被标记为垃圾邮件。
删除图标	从列表中删除 IP 地址。
编辑图标	点击编辑“邮件地址”“匹配类型”与“动作”项。
移动图标	点击在列表中移动条目。防火墙是以列表中显示条目的顺序执行操作的。例如，IP 地址 1.1.1.1 列为垃圾地址，1.1.1.0 为干净的邮件，您必须将地址 1.1.1.1.置于 1.1.1.0 至上，才可以生效。

27.4.3 配置反垃圾邮件的 IP 地址列表

进入反垃圾邮件>黑/白名单>IP 地址，点击“新建”在 IP 地址列表中添加新的 IP 地址。使用以下两种格式输入 IP 地址与掩码：

- x.x.x.x，例如 62.128.69.100
- x.x.x.x/x.x.x.x，例如 62.128.69.100/255.255.255.0
- x.x.x.x/x，例如 62.128.69.100/24

增加IP地址	
IP地址/子网掩码	
动作	标记为垃圾邮件
启用	☑
确定	取消

图27.4-4　添加 IP 地址

参数信息

参数名称	参数说明
IP 地址/掩码	输入 IP 地址与掩码。
插入	选择 IP 地址放置的位置。
动作	设置动作。标注为垃圾邮件，执行内容保护表配置的处理方式；标注为干净邮件继续执行其它的过滤项；或标注为拒绝（只适用于 SMTP）丢弃该会话。
启动	选中该功能框，使该地址生效。配置反垃圾邮件的邮件地址列表您可以添加多个反垃圾邮件地址列表，并对每个保护内容表设置最合适

参数名称	参数说明
	的地址列表。进入垃圾邮件过滤>黑/白名单>邮件地址，并点击“新建”在邮件地址列表中添加新的邮件地址或域名。

IP地址　E-mail地址
新建
名称　#条目　保护内容表　注释

图27.4-5　添加邮件地址

参数信息

参数名称	参数说明
添加	在目录中添加新的列表，输入列表名称并点击添加。新建的列表在默认情况下是空的。
名称	可用的反垃圾邮件邮件地址名单。
#条目	列表中每个项目的编号。
内容保护表	每个邮件地址列表应用的内容保护列表。
注释	作为可选项，对每个邮件地址列表添加描述内容。
删除图标	点击从目录中删除邮件地址列表。如果该列表应用于内容保护列表将不能被删除。
编辑图标	点击编辑邮件地址列表的“列表名称”以及“描述”项。

创建新的反垃圾邮件地址列表进入反垃圾邮件>黑/白名单>e-mail 地址，并点击“新建”在反垃圾邮件地址列表目录中添加邮件地址列表。

新列表
名称
注释　(最大63个字符)
确定　取消

图27.4-6　新建垃圾邮件地址列表

参数信息

参数名称	参数说明
名称	输入新建列表的名称。
注释	如需要，输入对该列表描述性的内容。

27.4.4 查看垃圾邮件地址列表

您可以配置 ZXSEC US 设备过滤某一特定发送人发送的邮件，或是某一个域名（如 example.net）发送的所有邮件。可以将每个邮件地址标注为干净，垃圾邮件或拒绝选项。

进入反垃圾邮件>黑/白名单>e-mail 地址，查看 ZXSEC US 设备的 IP 地址列表。

垃圾邮件地址列表

参数信息

参数名称	参数说明
名称	邮件地址列表名称。在名称字段输入输入新的名称，点击 ok 确认可以生成新的列表名称。
注释	可选项。在描述字段中添加或编辑描述性信息。
新建	在邮件地址列表中添加新的地址。
全部	列表中条目的数量。
翻上页图标	点击查看上一页信息。
翻下页图标	点击查看下一页信息。
清除全部	点击清除全部列表信息。
邮件地址	当前列表的邮件地址。
匹配类型	邮件地址条目应用的匹配类型。使用通配符或常规表达式。详细信息，参见“使用正则表示式”。
动作	对与地址列表匹配的地址所采取的动作；标注为垃圾邮件，实行保护内容表中对垃圾邮件的处理方法；标注为干净邮件，允许该邮件通过下一过滤项。
删除图标	从列表中删除邮件地址。
编辑图标	点击编辑“邮件地址”“匹配类型”与“动作”项。
移动图标	点击在列表中移动条目。防火墙是按照列表所列条目的顺序执行操作的。例如,您将 abc@abc.com 列表为干净的地址且将*@abc.com 设置为垃圾邮件，您必须将 abc@abc.com 列于*@abc.com 之上。

27.4.5 配置垃圾邮件地址列表

进入反垃圾>黑/白名单>e-mail 地址，在列表中添加邮件地址或域名。

增加邮件地址
邮件地址
模板类型 匹配码
动作 标记为垃圾邮件
启用
确定 取消

图27.4-7 添加邮件地址

参数信息

参数名称	参数说明
邮件地址	输入邮件地址。
匹配类型	选择匹配类型：通配符或正则表达式。
插入	选择该邮件地址在列表中放置的位置。
动作	对该地址采取的动作 标注为垃圾邮件，实行保护内容表中对垃圾邮件的处理方法。 标注为干净邮件，允许该邮件通过下一过滤项。
启动	选中该功能框，使该邮件地址生效。

1. 输入添加的邮件地址或匹配类型。
2. 选择列表条目的匹配类型。
3. 如需要，选中“之前”或“之后”将所添加的邮件地址放置在列表中正确的位置。
4. 选择对新添加的邮件地址所采取的动作。
5. 选中“启动”功能框。
6. 点击 OK 确认。

27.5 垃圾邮件过滤功能的高级配置选项

反垃圾功能的高级配置选项是指那些只有通过 CLI 命令配置，在基于 web 的管理器不能进行配置的功能项。有关如何使用 CLI 命令的详细信息，参见 US 设备 CLI 使用参考手册。

config spamfilter mheader

使用该命令配置邮件信息基于 MIME 标头过滤。在每一项内容保护配置列表项中启动 MIME 标头过滤。

ZXSEC US 设备将向内邮件与配置的 MIME 标头密钥与标头值进行逐个匹配。如果发现匹配选项，对应的保护设置文件将对邮件采取动作。如果发现匹配，该邮件将被过滤到下一项垃圾邮件过滤选项。

MIME（多用途的网际扩充协议）标头是添加在邮件中说明内容类型以及内容编码的描述，如邮件正文的文本类型或生成邮件的程序。MIME 标头举例：

- X-mailer: outgluck
- X-Distribution: bulk
- Content_Type: text/html
- Content_Type: image/jpg

MIME 标头的第一部分叫做标头密钥或就是标头。第二部分叫做标头值。垃圾邮件发送人一般在标头值中插入注解或保持该值为空白。这些异常的标头通常用于蒙蔽垃圾邮件过滤或病毒检测功能。

您可以使用 MIME 标头列表识别一些垃圾邮件信息中包含的某些大宗邮件程序或某些类型的内容。您可以对与配置的每项标头相配置的邮件采取的动作，如标注为干净或垃圾邮件。

config spamfilter dnsbl

使用该命令配置邮件信息使用 DNSBL（基于 DNS 黑洞列表）与 ORDBL（开放中继数据库列表）过滤。在每一项内容保护配置列表项中启动 DNSBL 与 ORDBL 过滤。

ZXSEC US 设备将邮件发送人的 IP 地址或域名与配置的数据库列表进行匹配。ZXSEC US 设备同事在列表中检索所有的服务器。如果发现匹配选项，对应的保护设置文件将对邮件采取动作。如果发现匹配，该邮件将被过滤到下一项垃圾邮件过滤选项。

使用 DNSBL（基于 DNS 黑洞列表）与 ORDBL（开放中继数据库列表）是较为高效的方法过滤进入系统邮件并识别以及采取动作标注为垃圾邮件或拒绝邮件。这些列表作为域名服务器，将向内邮件的域名与列表中已知的发送垃圾邮件的地址进行匹配，或允许垃圾邮件通过。DNSBL 追踪被报告为垃圾邮件的源地址，ORDBL 追踪不安全的第三方 SMTP 服务器，也称为开放中继，一些垃圾邮件发放者使用开放中继发送未经请求的大宗邮件。



注意：

有几台免费的签订的服务器用于对访问并更新 DNSBL 与 ORDBL 列表。检查您所使用的服务并确认连接到服务器域名的正确性。

由于 ZXSEC US 设备使用服务器域名连接到 DNSBL 或 ORDBL 服务器，DNS 服务器中必须能够查找到该域名。

27.6 Perl 正则表达式

邮件地址列表，MIME 标头列表以及禁忌词汇列表的条目中都可以使用包含通配符与 Perl 正则表达式。

有关如何使用 Perl 正则表达式的详细信息，参见 http://www.perldoc.com5.8.0./pod/perlre.html

27.6.1 正则表达式与通配符匹配模式

Perl 正则表达式中，“•”表示任何的单独的字符。类型通配符匹配模式中的“？”。

- zte.com.cn 不仅与 ZTEcom.cn 相匹配，而且与所有含有 zte.com 的词汇相匹配。与特殊的字符如“.”与“*”相匹配，使用转义字符“\”。
- 与 zte.com.cn 相匹配，常规表达式应该是:zte.com.cn Perl 正则表达式中，“*”表示与在列出的词汇中重复出现的字符的匹配。例如 US*\.com 与 USiii.com 相匹配，不是与 zte.com.cn 匹配。与任何字符匹配多次，使用“.”“.”表示与任何字符匹配，“*”表示在匹配词汇中出现一次或多次的字符。例如，通配符匹配模式 US*.com 应该是 for.*\.com.。

27.6.2 词界

Perl 正则表达式中，模式没有确定的词界。例如，常规表达式“test”不仅与“test”相匹配，而且与任何包含有 test 的词组相匹配，如 atest，mytest，testimony 以及 atestb 等。“\b”符号表示词界。与 test 进行精确匹配，表达式应该为\btest\b。

27.6.3 大小写

常规表达式模式匹配在网页与垃圾邮件过滤选项中是需要大小写精确的查询。配置使禁忌词汇成为不敏感匹配，使用常规表达式/i.例如，/bad language/I 将屏蔽所有含有 bad language 的全部邮件。

Perl 正则表达式格式

表达式	匹配
abc	abc(按字符顺序精确匹配，但该字符串可以在词句中任何位置)
^abc	abc 在字符串开头
abc$	abc 在字符串结尾
a|b	字符串含有 a 或 b
^abc|abc$	abc 在字符串的开头或者结尾
ab{2,4}c	一个 a 之后接两个、三个或四个 b，再接一个 c
ab{2,}c	一个 a 之后接至少两个 b，再接一个 c
ab*c	一个 a 之后接 0 个或更多个 b，再接一个 c
ab+c	一个 a 之后接一个或更多个 b，再接一个 c
ab?c	一个 a 之后接 0 个或 1 个 b，再接一个 c。也就是 abc 或 ac
a.c	一个 a 之后接任一单个字符（不换行），再接一个 c
[abc]	字符串含有 a,b 或 c 中任一个
[Aa]bc	字符串含有 Abc 或 abc
[abc]+	由 a,b 和 c 中的一个或多个组成的任意非空字符串
[^abc]+	不含 a,b 和 c 中任何一个的非空字符串（如 defg）
\d\d	匹配任意一个两位数，如 42。也可表达为\d{2}
/i	进行忽略大小写的匹配。例如，/bad language/i 匹配任何大小写形式的 bad language。
\w+一个词	匹配一个由数字、英文字母和下划线组成的字符串，如 foo,12bar8 及 foo_1
100\s*mk	匹配 100 和 mk 之间有 0 个或任意多个空白的字符串。（空白包括空格，tab 间隔和换行）
abc\b	abc 之后为词界（例如，abc！能匹配，而 abcd 不能）
perl\B	perl 之后非单词边界（例如，perlet 能匹配，而 perl stuff 不能）
\x	使正则表达式分析器忽略既不在反斜杠后，又非字符的空白。可用于将正则表达式分成更具可读性的多个部分。
/x	用于在其他文本中插入正则表达式。如果模式首字符前有斜线'/'，斜线将被用作分隔符。模式中必须有另外一个斜线，两个斜线之间的部分会被当作正则表达式，而第二个斜线之后的部分会被解析为各种正则表达式选项（'i','x',等等）。缺少第二个斜线会引起错误。在正则表达式中，首尾的空格都会被当成表达式的一部分。

举例

在词汇屏蔽任何词

/block|any|word/

屏蔽故意拼错的词垃圾邮件发送者通常在在单词中故意插入其它字符以蒙骗垃圾邮件屏蔽软件。

/^.*v.*i.*a.*g.*r.*a.*$/i

/cr[eéèêë][\+\-*=<>\.\,;!\?%& § @\^° \$£€ \{\}()\[\]\|_01]dit/I 屏蔽通常垃圾邮件中包含的词语以下列出的是垃圾邮件信息中通常使用的信息。

/try it for free/i

/student loans/i

/you’re already approved/i

/special[\+\-*=<>\.\,;!\?%&~#§@\^°\$£€\{\}()\[\]\|_1]offer/i

第28章 IM/P2P & VoIP

28.1 概述

描述

IM/P2P&VoIP 菜单是有关即时通讯的用户管理工具以及网络中使用 IM，P2P 以及 VoIP 功能的状态说明。IM，P2P 与 VoIP 必须在活动的内容保护列表中启动才能够生效。

内容

28.2 IM/P2P & VoIP

即时消息（IM: instant messenger），端到端（Peer to peer）与基于互联网协议的语音通讯（Voice over Internet Protocol）作为互联网上个体之间的实时通讯工具获得广泛的使用。一些公司甚至倚赖 IM 用于重要的业务流程，如客户/技术支持。

现在来讲最常使用的 IM 协议包括 AOL 即时通讯、Yahoo 即时通讯工具、MSN 以及 ICQ。虽然这已经是为数不少较为常用的 IM 工具，但是仍然有很多协议正在被开发或这些旧的 IM 工具不断的升级。

P2P 协议常用于用户之间文件的传输，这样的传输比较占用带宽。VoIP 正在被更多的公司使用。VoIP 大大的降低了长话通讯的费用。一些公司限制 IM/P2P 与 VoIP 的使用，为了更有效的管理带宽。USOS 系统下，您可以控制与监控 IM/P2P 与 VoIP 的使用。

USOS 支持两种 VoIP 协议：SIP（SIP:Session Initiation Protocol）与 SCCP（SCCP:Skinny Client Control Protocol）。

中兴通讯认为合理的利用 IM/P2P 可以协助公司的业务发展，但是，如果滥用便降低了工作率以及网络性能。

ZXSEC US 设备允许设置建立用户列表，允许或屏蔽这些程序的使用以及使用的带宽限制。

通过将所设置的保护策略与简明的统计报告结合，您可以知道应用了怎样的程序以及所应用程序的目的，从而有效地控制 IM/P2P 程序，提高效率。

USOS 系统中有所支持的 IM/P2P 协议列表，并保持从 ZTE Distribution Network 更新可用的协议。不必等到固件升级并可以有可用的最新协议更新。同时，USOS 同时也提供方法处理在协议升级之前出现的未知协议。

下表所列为当前 USOS 识别的 IM/P2P 应用程序。列表中同时也包括解码器、与解码器有关的应用程序，以及 ZXSEC US 接口中解码器的位置。



注意：

下表中被标注为黑体的应用程序可以连接到多个 P2P 网络。启动 IM 与 P2P 解码器与特征可以提高 IPS 性能。例如，如果您想应用 IPS，同时不屏蔽 IM 或 P2P 程序，您应该启动 IM/P2P 解码器与特征。常规情况下，如果您关闭其他特征，系统性能会更好，但是对于 IM/P2P，情况刚好相反。

USOS 3.0 支持的 IM/P2P 程序

IPS	应用程序
即时通讯	
AIM（防火墙>保护内容表>IM/P2P）	AIM,AIM Triton, ICQ
I CQ（防火墙>保护内容表>IM/P2P）	
MSN（防火墙>保护内容表>IM/P2P）	MSN Messenger
qq（入侵保护>特征>协议解码器>im_decoder）	QQ
Yahoo!（防火墙>保护内容表>IM/P2P）	Yahoo Messenger
msn_web_messenger（入侵保护>特征>协议解码器>im_decoder）	MSN web Messenger
google_talk（入侵保护>特征>协议解码器>im_decoder）	Google Instant Messenger
rediff（入侵保护>特征>协议解码器>im_decoder）	Rediff Instant Messenger
BitTorrent（防火墙>保护内容表>IM/P2P）	BitComet Bitspirit Azureus Shareazae
Donkey（防火墙>保护内容表>IM/P2P）	eMule Overnet

IPS	应用程序
	Edonkey2k Shareaza Bearshare MLdonkey iMesh
Gnutella（防火墙>保护内容表>IM/P2P）	Bearshare Shareaza LimeWire Xolox Swapper iMesh MLdonkey Gnucleus Morpheus Openext Mutella Qtella Qcquisition Acquisition NapShare gtk-gnutella
KaZaA（防火墙>保护内容表>IM/P2P）	KaZaA
Skype（防火墙>保护内容表>IM/P2P）	Skype
WinNY（防火墙>保护内容表>IM/P2P）	WinNY
ares（入侵保护>特征>协议解码器>p2p_decoder）	Ares Galaxy
direct_connect（入侵保护>特征>协议解码器>p2p_decoder）	DC++

28.3 配置 IM/P2P 协议

不同的公司对配置 IM/P2P 要求不同，需要配置不同的策略。ZXSEC US 设备提供如您所愿的配置服务。

28.3.1 怎样启动与撤消 IM/P2P 选项

以下是启动或撤消 IM/P2P 选项的四个配置位置。同时，有关如何启动预先定义 的特征、用户定义的特征或未知用户策略。

在入侵保护中启动预先定义的 IM/P2P 特征，步骤如下。

1. 进入“入侵保护>特征>预定义”。

2. 使用特征组过滤器搜索 IM 与 P2P 特征。
3. 选中功能框启动特征。
4. 选中日志功能，启动对特征进行日志记录。
5. 查看特征对应的行，点击编辑。
6. 设置动作与严重性级别。
7. 点击 OK 确认。

对未知协议创建用户定义的 IM/P2P 特征

1. 进入“入侵保护>特征>用户定义>新建”。
2. 输入特征的名称。
3. 输入特征。
4. 设置严重性级别与动作。
5. 点击 OK 确认。

对未知 IM 用户创建策略

1. 进入“IM,P2P&VoIP>用户>配置”。
2. 对四项 IM 程序设置允许或屏蔽。
3. 点击应用。

28.3.2 如何在保护内容表配置 IM/P2P/VoIP 选项

在保护内容表中有几个区域可以配置 IM/P2P/VoIP 选项，详细信息参见本手册中防火墙保护内容表章节以及 IM/P2P/VoIP 技术手册。

如何配置旧版本的 IM/P2P 程序

一些旧版本的 IM/P2P 协议可以绕过文件屏蔽功能，因为信息类型不能被识别。

ZXSEC US 设备支持的 IM 协议包括：

- MSN 6.0 以及以上版本
- ICQ 4.0 以及以上版本
- AIM 5.0 以及以上版本
- Yahoo 6.0 以及以上版本

如果您想设置屏蔽比以上所述协议更旧的版本，可以使用 CLI 命令 config imp2p old-version.详细信息参见 ZXSEC US 设备 CLI 使用参考手册。

怎样配置系统不支持的协议

如果您发现一项协议是系统所不支持，请先确定 IPS 数据包是否已经更新。如果 IPS 已经更新，仍然发现系统所不支持的协议，这时您可以使用用户定义特征。

创建用户定义特征

1. 进入“入侵保护>特征>用户定义>新建”。
2. 输入特征的名称。
3. 输入特征。
4. 设置严重性级别与动作。
5. 点击 OK 确认。



注意：

需要检测新的 IM/P2P 或是否存在新的协议版本时，您只需要通过 US SERVICE 中心（US SERVICE 中心:ZTE Distribution Network）更新 IPS 数据包。不需要升级固件。

28.4 统计信息列表

系统管理员可以查看即时通讯以及点对点传输协议在网络中使用的状况。统计表信息是有关 IM 与 P2P 使用情况的概览图，以及每项 IM 协议使用的情况。



注意：

如果 ZXSEC US 设备设置使用了虚拟域，IM/P2P 功能可以进行全局配置。在主菜单中点击“全局配置”，查看该功能项。

28.4.1 查看统计信息列表

统计信息列表提供所有 IM，P2P 与 VoIP 协议的信息。进入 IM/P2P>统计表>概述，查看 IM/P2P 的使用情况信息。

摘要 协议

自动刷新的间隔 5 seconds 刷新 使用的起始日期: 2008-06-03 15:49:26 重置统计

IM使用率	MSN	Yahoo!	AIM	ICQ
用户				
连接的用户	0	0	0	0
从上次重置起计	0	0	0	0
阻断	0	0	0	0
交谈				
总的交谈会话数	0	0	0	0
总的信息	0	0	0	0
传输的文件				
从上次重置起计	0	0	0	0
阻断	0	0	0	0
语音交谈				
从上次重置起计	0	0	0	0
阻断	0	0	0	0

P2P使用率	BitTorrent	eDonkey	Gnutella	KaZaa	WinNY
P2P使用率					
总的字节数	0.00 B	0.00 B	0.00 B	0.00 B	0.00 B
平均带宽	0.00 B/s	0.00 B/s	0.00 B/s	0.00 B/s	0.00 B/s

VoIP使用率	SIP	SCCP
线程		
活动线程 （电话连接，等等）	0	0
通话		
所有通话（从上一次复位）	0	0
通话失败/丢弃	0	0
通话成功	0	0

图28.4-1 IM/P2P/VoIP 统计信息

参数信息

参数名称	参数说明
自动刷新的间隔	设置自动刷新信息表的时间间隔。该间隔时间可以设置为“无间隔刷新”到 30 秒之内任何时间间隔这样的刷新频率。
刷新	点击刷新到最新的数据信息。
重置统计表	点击将统计表归零。
用户	对于每项 IM 协议，列出以下用户信息。 ● 当前用户 ● 上一次重置后的用户 ● 被屏蔽的用户
聊天信息	对于每项 IM 协议，列出使用该协议进行的聊天信息。聊天绘画总数与信息量总数。
文件传输	对于每项 IM 协议，列出使用该协议进行的文件传输。上一次重置后信息传输量与被屏蔽的文件传输。
语音聊天	对于每项 IM 协议，列出使用该协议进行的语音聊天信息。上一次重置后语音信息与被屏蔽的语音聊天信息。
P2P 使用情况	对于每项 P2P 协议，列出该协议的使用情况。 传输文件的总字节数 使用的平均带宽
VoIP 使用率	对于 SIP 与 SCCP 协议，列出以下信息：

参数名称	参数说明
	● 活动的会话（连接的呼叫） ● 呼叫总数（从最近一次重启后） ● 失败的呼叫/丢弃 ● 成功的呼叫

根据协议查看统计信息列表

您可以查看每项 IM 协议的使用情况。进入 IM/P2P>统计表>协议，查看各项协议使用的情况。

您可以启动记录 IM 聊天信息以及设置各种限制选项。



图28.4-2 IM 信息状态图

参数信息

参数名称	参数说明
自动刷新的间隔	设置自动刷新信息表的时间间隔。该间隔时间可以设置为“无间隔刷新”到 30 秒之内任何时间间隔这样的刷新频率。
协议	点击选择所有显示 AIM,ICQ,MSN 或 Yahoo 之中哪项协议的使用情况。
用户	针对设置查看的协议，列出以下用户信息。当前用户，上一次重置后的用户以及被屏蔽的用户。
设置	针对设置查看的协议，列出使用该协议进行的聊天信息。聊天绘画总数与信息量总数。

参数名称	参数说明
信息	针对设置查看的协议，列出以下消息数据。信息总数，发送的消息，接收的消息。
传输的文件	针对设置查看的协议，列出使用该协议进行的文件传输。上一次重置后信息传输量与被屏蔽的文件传输。
语音聊天	针对设置查看的协议，列出使用该协议进行的语音聊天信息。上一次重置后语音信息与被屏蔽的语音聊天信息。

28.5 用户

当 IM 用户通过防火墙连接，ZXSEC US 设备将在当前用户列表中显示哪个用户已经连接登录。管理员可以根据该列表设置允许或屏蔽该用户。也可以针对未知的用户设置防火墙策略进行处理。



注意：

如果 ZXSEC US 设备设置使用了虚拟域，IM/P2P 功能可以进行全局配置。在主菜单中点击“全局配置”，查看该功能项。

28.5.1 查看当前用户列表

当前用户列表显示当前已连接的使用即时通讯的用户。进入 IM/P2P/VoIP>用户>当前用户，查看当前用户信息。

当前用户 用户列表 配置

协议: All

#	协议	用户名	源IP	最后登录时间

图28.5-1 当前用户列表

当前用户列表的参数信息：

参数名称	参数说明
协议	设置显示使用 AIM,MSN,ICQ 或 Yahoo 协议的当前用户。设置为“全部”将显示所有当前的用户。
使用协议	当前用户使用的协议。
用户名	注册使用 IM 协议时用户所选择的名称。多个 IM 协议可以使用相同的用户名。每个用户名与协议成对分别显示在列表中。
源 IP 地址	用户使用的发起 IM 会话的 IP 地址。

参数名称	参数说明
最后登录时间	当前用户使用 IM 协议最后一次登录的时间。
屏蔽	设置强制屏蔽用户并将用户放入永久性黑名单中。管理员必须明确设置所用屏蔽用户的用户名以及使用的协议。

28.5.2 查看用户列表

用户列表显示被允许访问即时通讯服务的用户（白名单内的用户）或不在被即时通讯服务屏蔽的用户。

进入 IM/P2P/VoIP>用户>用户列表，显示用户列表。在临时用户列表中点击“新建”可以添加用户。

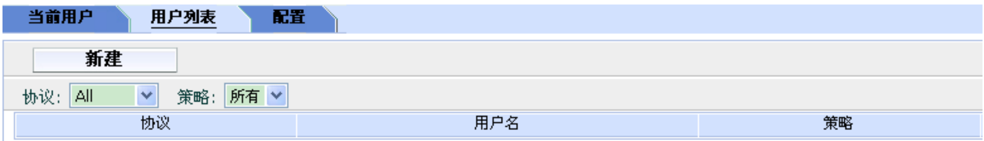


图28.5-2　用户列表

当前用户列表的参数信息：

参数名称	参数说明
新建	点击在列表中“新建”用户。
协议	设置显示使用 AIM,MSN,ICQ 或 Yahoo 协议的当前用户。设置为“全部”将显示所有当前的用户。
策略	设置过滤策略：允许、拒绝或全部。
使用协议	当前用户使用的协议。
用户名	注册使用 IM 协议时用户所选择的名称。多个 IM 协议可以使用相同的用户名。每个用户名与协议成对分别显示在列表中。
策略	设置用户使用 IM 协议登录时系统设置的动作：屏蔽或拒绝。
编辑图标	更改以下用户信息：协议、用户名或策略。
删除图标	将用户从列表永久删除。

28.5.3 在用户列表中添加新的用户

在用户列表中添加新的用户，设置允许或屏蔽该用户访问即时通讯服务。进入 IM/P2P/VoIP＞用户＞用户列表，点击“新建”添加用户。

编辑用户

协议 AIM

用户名

策略 阻断

确定 取消

图28.5-3 编辑用户

参数信息：

参数名称	参数说明
协议	从下拉菜单中选择即时通讯协议：AIM,ICQ,MSN,Yahoo.
用户名	输入用户名。
策略	从下拉菜单中选择策略：允许或阻断。

对未知 IM 用户配置策略

对未知用户设置用户策略以决定对未知用户所采取的处理动作。可以设置未知用户能够使用部分或不全的 IM 协议或将用户添加在白名单中，或者屏蔽未知用户使用部分或全部 IM 协议将其放置在黑名单中。管理员可以查看黑白名单并将用户添加在用户名单中。

进入 IM/P2P/VoIP＞用户＞配置，配置 IM 策略。

用户策略

当未知的IM用户连接要穿越防火墙时，应该采用下面的操作：

	MSN	Yahoo!	AIM	ICQ
自动允许	○	○	○	○
自动阻断	◉	◉	◉	◉

临时用户列表 协议：All

#	协议	用户名	策略

应用

图28.5-4 IM 用户策略

配置或查看 I M用户策略的以下设置选项：

参数信息：

参数名称	参数说明
自动允许	设置允许未知用户访问的 IM 协议。将未知用户添加在临时性白名单中。
自动阻断	设置拒绝未知用户访问的 IM 协议。将未知用户添加在临时性黑名单中。
临时用户列表	添加在临时性黑白名单中的新用户。用户信息包括：协议、用户名以及对该用户应用的策略。 **注意：** ZXSEC US 设备重启后，该名单将被清除。
协议	设置显示使用 AIM，ICQ，MSN 或 Yahoo 协议的当前用户。设置为“全部”将显示所有当前的用户。
用户名	注册使用 IM 协议时用户所选择的名称。多个 IM 协议可以使用相同的用户名。每个用户名与协议成对分别显示在列表中。
策略	设置用户使用 IM 协议登录时系统设置的动作：屏蔽或拒绝。
永久性允许	点击将用户添加到永久性白名单中。用户的状态仍然在线并在 IM/P2P/VoIP＞用户＞用户列表中显示。
永久性拒绝	点击将用户添加到永久性黑名单中。用户被强制离线并在 IM/P2P/VoIP＞用户＞用户列表中显示。
应用	点击“应用”是全局用户策略配置生效。

第29章 日志与报告

29.1 概述

描述

本章是有关如何启动日志记录功能、查看日志文件以及通过 web 管理器查看报告的内容描述。ZXSEC US 设备提供了较为宽泛的日志记录功能，能够记录如网络流量，系统以及网络内容保护表的日志。通过详细的日志信息与报告可以对历史状态以及当前状态的网络活动进行分析，有助于识别涉及网络安全性的问题，减少网络的误用与滥用。



注意：

US OS3.0MR5 中，VDOM 的设置可能会影响日志记录与报告功能；在配置使用这些功能之前，请先确认进入 VDOM 中是否可以访问日志记录与报告功能。

内容

29.2 ZXSEC US 设备日志记录功能

ZXSEC US 设备可以配置记录不同网络活动以及流量的日志，包括：

- 全部网络流量日志

- 与系统有关的事件日志,包括系统重启,HA 以及 VPN 活动
- 病毒扫描与屏蔽
- Web 过滤,URL 以及 HTTP 内容屏蔽
- 攻击特征以及异常检测与防护
- 垃圾邮件过滤
- 即时通讯以及点对点传输流量日志
- VoIP 呼叫日志

您可以定制 ZXSEC US 设备将这些日志记录为哪个级别的日志,以及日志存储的位置。ZXSEC US 设备可以将系统事件日志与网络入侵活动日志存储在系统内存中。但是由于内存本身具有的局限性，旧的日志信息将不能被保存，而且由于网络流量占用的内存空间较大，也不能被存储在内存中。

ZXSEC US 设备支持外部的日志存储设备 WebTrend 以及其他 Syslog 服务器。您也可以配置 ZXSEC US 设备将日志信息发送到配置到安装的硬盘中。

通过 ZXSEC US 设备，您可以配置从设备内存中或是 ZXSEC US 设备自配置的硬盘中查看网络活动的情况与日志。在日志文件中，您可以定制过滤选项方便查看具体的日志信息。



注意：

有关如何配置将日志存储到 ZXSEC US 设备可用的硬盘中的详细信息，参见 ZXSEC US 设备 CLI 使用手册。

有关日志信息存储的格式以及详细信息，参见 ZXSEC US 设备日志信息参考手册。

29.3 日志安全级别设置

您可以设置日志文件存储的位置，以及所要存储日志文件的级别。日志信息可以设置为不同的级别，ZXSEC US 设备记录您所设置的级别的以及该级别以上级别的日志信息。如表 43"日志的安全级别"说明，如果您将日志记录设置为记录"报错"，ZXSEC US 将记录包括"报错"级别以及该级别以上所有级别的日志信息。

日志安全级别设置参数信息：

级别	描述	产生源
0-紧急	致使系统不能够稳定运行。	事件日志，尤其是管理事件一般发出紧急级别日志。
1－告警	需要采取立即的行动措施。	攻击日志是唯一产生告警级别的日志信息。
2－严重	影响发挥模块设置的功能。	事件、反病毒与垃圾邮件过滤日志。
3－错误	存在错误信息，功能性受到影响。	事件与垃圾邮件过滤日志。
4－警示	功能性受到影响。	事件与垃圾邮件过滤日志。
5－通知	常规事件的通知。	流量与 web 过滤日志。
6－信息	有关系统操作的常规信息。	内存存储、事件与垃圾邮件过滤日志。

日志调试级别没有在表 44 中示出，因为很少被使用。这是日志信息的最低级别，通常是一些固件状态信息，如 ZXSEC US 设备不能正常工作时，可以参见该日志查找有关原因。调试日志信息只有在日志级别设置为调试时才会产生。调试日志信息可以由所有类型的 ZXSEC US 功能产生。

29.4 高可用性（HA）群集日志记录

当配置记录 HA 群集的日志时，需要配置主设备发送日志到 Syslog 服务器。该设置将应用于从属设备。从属设备先发送日志信息到主设备，然后主设备发送全部的日志到 Syslog 服务器。

29.5 日志存储

配置 ZXSEC US 设备将日志信息文件存储的位置。日志信息存储的类型及频率将决定您设置日志存储的类型。例如，系统内存中的日志信息存储空间有限，只有数量较小的信息可以存放在内存中。而且，由于流量日志以及内容日志占用较大的空间，ZXSEC US 设备将不能将流量日志信息存储在内存中。

如果 ZXSEC US 设备配置了硬盘，您也可以使用 CLI 命令配置将日志信息记录到硬盘中。相关的配置命令，参见 ZXSEC US 设备 CLI 使用参考手册。

如果您需要配置将日志信息记录到多个 Syslog 服务器，参见 ZXSEC US 设备 CLI 使用参考手册。

29.5.1 配置将日志存储在系统内存

ZXSEC US 系统内存容量有限并且只能够显示最近的日志条目。流量与内容日志不能够储存在内存的缓存中。当内存已满时，ZXSEC US 设备将以新的日志从最为原始的日志信息中进行覆盖存储。当 ZXSEC US 设备重新启动时，全部的日志条目都将被删除。

如果 ZXSEC US 设备配置了硬盘，使用 CLI 命令可以配置将日志记录到磁盘。

配置 ZXSEC US 设备将日志存储到系统内存

1. 进入日志与报告>日志配置>日志设置。
2. 点击“内存”。
3. 点击蓝色箭头扩展内存选项。
4. 选择所要存储日志的安全级别。

日志信息可以设置为不同的级别，ZXSEC US 设备记录您所设置的级别的以及该级别以上级别的日志信息。参见表 44 所示“日志的安全级别”说明。

29.5.2 配置将日志存储到 Syslog 服务器

Syslog 是远程运行 syslog 服务器的计算机设备。Syslog 是行业内共享的网络设备，用于捕获日志信息。Syslog 服务器是便捷灵活的日志设备，因为任何计算机设备均运行 syslog 软件，如 Linux，Unix 与基于 intel 的 Windows 系统。

配置将日志记录到 Syslog 服务器时，您需要配置日志文件的格式为常规或 CSV 格式。CVS 格式中文件以逗号分隔，常规格式使用空格。配置存储日志所属的设备，便于识别日志文件。

syslog服务器设置
名称/IP 10.16.13.12
端口 514
最低日志级别 信息
工具 local7
启用CSV格式

图29.5-1 将日志存储到 syslog 设备

配置 ZXSEC US 设备发送日志信息到 syslog 服务器

1. 进入日志与报告>日志配置>日志设置。
2. 点击“Syslog”。
3. 点击蓝色箭头扩展内存选项。
4. 设置以下 syslog 选项并点击“应用”。

参数信息：

参数名称	参数说明
名称/IP	存储日志的 syslog 服务器的域名或 IP 地址。
端口	与 syslog 服务器通讯的端口号，通常情况下是端口 514。
日志级别	日志信息可以设置为不同的级别，ZXSEC US 设备记录您所设置的级别的以及该级别以上级别的日志信息。如表 44 所示“日志的安全级别”说明。
工具	日志信息生成源。默认情况下，ZXSEC US 报告的设施为本地。您可以更改设施信息表明生成信息的不同的 ZXSEC US 设备。
启用 CSV 格式	如果您启动 CSV 格式，ZXSEC US 设备将以 Comma Separated Value（CSV）格式生成日志。如果您不启动该各式，ZXSEC US 将以纯文本文件各式生成日志文件。



注意：

如果配置了不止了一个 Syslog 服务器，Syslog 服务器与其设置显示在日志设置页面。使用 CLI 命令可以配置多个 Syslog 服务器。详细信息，参见 ZXSEC US 设备 CLI 使用参考手册。

29.5.3 配置将日志存储到 Web Trends

运行 NetIQ WebTrend firewall reportting server 的远程计算机。ZXSEC US 生成日志的各式符合 WebTrend Enhanced Log Format（WELF）并与 NetIQ WebTrends Security Reporting Center 2.0 与 Firewall Suite 4.1.兼容。

使用以下命令，配置 ZXSEC US 设备将日志信息发送到 web trend。输入以下命令：

```
config log webtrends setting set server <address_ipv4>
set status {disable | enable}
end
```

关键字与变量	描述	默认值
server <address_ipv4>	输入存储日志信息的 web trend 的 IP 地址	没有默认值
status {disable | enable}	输入 enable 启动将日志记录到 web trend 服务器。	Disable

举例：

该例子显示如何设置远程 webtrend 服务器的 IP 地址，并将日志发送到该服务器。

```
config log webtrends setting set status enable
  set server 220.210.200.190
end
```

有关发送到 web trend 服务器的日志类型的配置选项，参见 ZXSEC US 设备 CLI 使用参考手册中的日志章节。

29.6 日志类型

ZXSEC US 设备提供了较为宽泛的日志选项配置记录各种日志以监控您的网络活动以及安全。例如，您可以启动记录 IM/P2P 日志信息。这些日志信息将显示您所管理的网络中的拥护使用 IM/P2P 的情况。

以下是日志类型以及如何启动该类型的日志记录。配置记录日志之前，您必须先配置 ZXSEC US 设备存储该类型日志的位置。详细信息，参见“日志存储”。

29.6.1 流量日志

流量日志记录通过 ZXSEC US 接口的流量日志。您可以配置记录防火墙策略控制的流量以及源与目标地址之间的流量。您可以应用全部的设置，如会话与数据包日志。您可以配置应用以下过滤选项：

参数信息：

参数名称	参数说明
策略允许的流量	ZXSEC US 设备记录防火墙策略设置允许通过的全部流量。
违反策略的流量	ZXSEC US 设备记录违背防火墙策略的，防火墙策略不允许通过的流量。



注意：

记录流量日志信息时，您必须设置该项日志的安全级别为“通告”。流量日志生成的日志信息一般不高于“通告”级别的信息。如果启动了 VDOM 设置，确认 VDOM 是否允许被访问以及启动流量日志的记录。

启动记录流量日志流量日志是记录接口或 VLAN 子接口进出的任何流量的日志。您需要将日志的级别设置为“通告”或更低的级别。

启动记录接口或 VLAN 子接口的流量日志

1. 进入系统管理>网络>接口。
2. 点击接口对应的编辑图标。
3. 点击日志选项。
4. 点击 OK 确认设置。

启动记录防火墙策略流量日志防火墙策略流量日志是指根据内容保护列表记录防火墙策略允许或拒绝的流量日志。

启动记录防火墙策略流量日志

1. 进入防火墙>策略。
2. 点击双向流量的蓝色箭头扩展策略列表。
3. 点击策略对应的编辑图标，或点击“新建”创建新的防火墙策略。
4. 设置为“允许日志记录”并点击 OK 确认。

29.6.2 事件日志

事件日志记录管理与活动日志，如配置更改或添加 VPN 以及高可用性（HA）这样的事件。

启动记录事件日志

1. 进入日志与报告>日志配置>日志设置。
2. 点击配置以下选项：

参数信息：

参数名称	参数说明
系统活动事件	ZXSEC US 设备记录所有有关系统活动的事件日志，如 ping 服务器的故障检测或网关状态。
IPSec 协商事件	ZXSEC US 设备记录所有 IPSec 通信协商日志，如进程与错误报告。
DHCP 服务事件	ZXSEC US 设备记录所有 DHCP 事件日志，如 DHCP 请求与回应日志。
L2TP/PPTP/PPPoE 服务事件	ZXSEC US 设备记录所有协议有关的事件日志，如管理器与 socket 创建进程。
管理员事件	ZXSEC US 设备记录全部管理性事件日志，如用户登录，重启与配置更新。
HA 活动事件	ZXSEC US 设备记录全部高可用性事件日志，如链接，HA 成员与状态信息。
防火墙认证事件	ZXSEC US 设备记录全部有关防火墙有关的事件日志，如用户认证。
模式更新事件	ZXSEC US 设备记录所有模式更新的事件日志，如反病毒与 IPS 模式更新以及更新失败的事件信息。
SSL VPN 用户验证事件	ZXSEC US 设备记录建立 SSL VPN 连接时所有用户验证事件的日志，例如用户登录与退出以及超时退出。
SSL VPN 管理员事件	ZXSEC US 设备记录有关 SSL VPN 的所有管理员事件日志，例如 SSL 配置以及 CA 证书下载与删除。
SSL VPN 通信会话事件	ZXSEC US 设备记录所有通信会话活动日志，例如应用程序启 动与屏蔽，超时以及验证等。

29.6.3 反病毒日志

记录在 web，FTP 或邮件流量中发生的病毒事件日志，如 ZXSEC US 设备检测到受病毒感染的文件类型或屏蔽超大的文件或邮件事件。您可以配置以下过滤选项：

参数信息：

参数名称	参数说明
病毒感染文件	ZXSEC US 设备记录所有受病毒感染的文件或邮件信息。
屏蔽文件	ZXSEC US 设备记录全部被屏蔽的文件事件信息。
超大文件/邮件传输	ZXSEC US 设备记录所有的超大文件或邮件传输的日志信息。
AV 监控	ZXSEC US 设备记录所有受病毒感染、屏蔽以及超大文件或邮件的传输日志。该功能可以应用于 HTTP、FTP、IMAP、POP3、SMTP 以及 IM 流量。

启动记录反病毒日志

1. 进入防火墙>内容保护列表。

2. 点击内容保护项对应的编辑图标。

3. 点击蓝色箭头扩展日志记录选项。

4. 选择记录反病毒事件日志，并点击 OK 确认。

29.6.4 网页过滤日志

网页过滤日志记录 HTTP US Service 网页分类错误信息以及内容屏蔽动作。

启动网页过滤日志选项

1. 进入防火墙>内容保护列表。

2. 点击内容保护项对应的编辑图标。

3. 点击蓝色箭头扩展日志记录选项。

4. 在 web 过滤选项下，启动 web 过滤事件日志记录。

5. 选择记录 US Service web 过滤网页分类错误信息（只适用于 HTTP）。

6. 点击 OK 确认。

29.6.5 攻击日志

攻击日志记录 ZXSEC US 设备检测发现并预防的攻击事件日志。您可以配置以下过滤选项：

参数信息：

参数名称	参数说明
攻击特征	ZXSEC US 记录根据攻击特征所检测发现并预防的攻击信息日志。
攻击异常	ZXSEC US 设备记录根据未知以及可疑流量模式检测并预防的攻击信息，以及 ZXSEC US 所采取动作的日志。

1. 进入防火墙>内容保护列表。

2. 点击内容保护项对应的编辑图标。

3. 点击蓝色箭头扩展日志记录选项。

4. 选择“入侵日志”并点击 OK 确认。



注意：

您必须确定攻击特征与攻击异常特征设置中启动了攻击日志记录选项。特征记录的日志选项是 ZXSEC US 设备默认的设置。确定用户定义的特征选项也启动了日志记录设置。详细信息，参见“入侵检测保护”。

29.6.6 垃圾邮件过滤日志

记录根据 SMTP，IMAP 与 POP3 流量中邮件地址模式检测为垃圾邮件的信息日志。

启动垃圾邮件日志记录

1. 进入防火墙>内容保护列表。
2. 点击内容保护项对应的编辑图标。
3. 点击蓝色箭头扩展日志记录选项。
4. 选择“垃圾邮件日志”并点击 OK 确认。

29.6.7 IM 与 P2P 日志

即时通讯（IM）以及点对点（P2P）记录即时消息文本信息以及音频通讯、文件传输以及传输日志、以及用户使用的 IM 应用程序以及传输内容信息的日志。

启动 IM 与 P2P 日志记录

1. 进入防火墙>内容保护列表。
2. 点击内容保护项对应的编辑图标。
3. 点击蓝色箭头扩展日志记录选项。
4. 选择“IM 活动”与“P2P 活动”并点击 OK 确认。

29.6.8 VoIP 日志

您可以启动记录 VoIP（VoIP: Voice over Internet Protocol）日志。您也可以对 SIP 与 SCCP 或 Skinny 协议配置 VoIP 速率限制。SIP 与 SCCP 是 VoIP 协议的两种类型。

通常 SCCP 与 SIP 的速率限制不同。对于 SIP，速率限制是对 SIP 流量通过 ZXSEC US 设备的限制。对于 SCCP，呼叫建立时间是 ZXSEC US 设备与用户端之间的过程，因为呼叫管理器通常是置于从用户端角度讲的 ZXSEC US 设备的相对的一边。

启动 VoIP 日志记录

1. 进入防火墙>内容保护列表。
2. 点击内容保护项对应的编辑图标。
3. 点击蓝色箭头扩展日志记录选项。
4. 选择“VoIP 活动”并点击 OK 确认。

配置 VoIP 活动

1. 进入防火墙>内容保护列表。
2. 点击内容保护项对应的编辑图标。
3. 点击蓝色箭头扩展 VoIP 选项。
4. 选中 SIP 与 SCCP 功能框。
5. 在“限制 REGISTER 请求”（请求/秒）（只适用于 SIP）字段输入每秒限制的请求数量。
6. 在“限制 INVITE 请求”（请求/秒）（只适用于 SIP）字段输入每秒限制的请求数量。
7. 在“限制呼叫建立”（请求/秒）（只适用于 SCCP）字段输入每分钟最大的呼叫数量。
8. 点击 OK 确认。

29.7 访问日志

访问日志提供了对存储在 ZXSEC US 硬盘或内存缓存中日志信息访问的功能。

通过日志访问菜单访问日志。日志访问菜单提供对存储在设备内存，硬盘日志的访问功能栏。每项功能栏中提供日志信息查看的功能选项，以及搜索与过滤选项。

访问内存中存储的日志文件

从日志访问页面，您可以查看存储在 ZXSEC US 硬盘中的日志文件。流量日志需要占用较大的存储空间，不存储在内存中。

访问 ZXSEC US 硬盘中的日志文件

1. 进入日志与报告>访问日志。
2. 选择所要访问日志的类型。

3. 从类型列表中选择硬盘。

访问存储在硬盘中日志信息

如果 ZXSEC US 设备配置了硬盘，您可以访问存储在 ZXSEC US 设备硬盘中的日志信息。日志访问的方法如同访问内存中存储日志的方法一样。您可以查看以及下载存储在硬盘中的日志信息。

1. 进入日志与报告>访问日志。
2. 选择所要访问日志的类型。
3. 从类型列表中选择硬盘。



图29.7-1 查看存储在 ZXSEC US 设备硬盘中的日志文件

日志类型点击选择您要查看的日志类型。一些日志文件如流量日志因为占用的存储空间较大不能够存储在 ZXSEC US 设备内存中。

参数信息：

参数名称	参数说明
文件名称	存储在 ZXSEC US 设备硬盘中的日志类型文件的名称。当一个日志文件达到存储的最大数量，
日志大小	日志文件的大小，以比特计。
最后一次访问时间	ZXSEC US 设备最近一次发送日志信息的时间。时间是以周月日年的格式显示，如周五、二月十六日十二点三十分五十四秒、二零零七年.
清除图标	清除当前的日志文件。清除当前日志文件将从活动的日志文件中删除所有当前的日志信息。日志文件不能被删除。
下载图标	点击下载日志文件或滚动日志文件。以文本格式或 CSV 格式下载日志文件。点击返回”链接图标返回页面。下载的日志文件只包括当前的日志信息。

参数名称	参数说明
查看图标	通过 web 管理器显示日志文件。
删除图标	删除滚动的日志文件。建议在删除滚动日志之前先要下载备份，因为滚动日志文件在删除后是不能再获取的。

29.8 查看日志信息

日志访问菜单中显示日志信息。日志访问菜单中显示存储在 ZXSEC US 设备内存、ZXSEC US 设备硬盘的选项栏。

栏目显示日志文件中的内容。日志访问页面的上面部分是页面导航功能栏，信息栏显示在日志文件中查找到的匹配内容，信息栏中的导航栏有助于您移动日志信息并确定查询的具体日志信息。

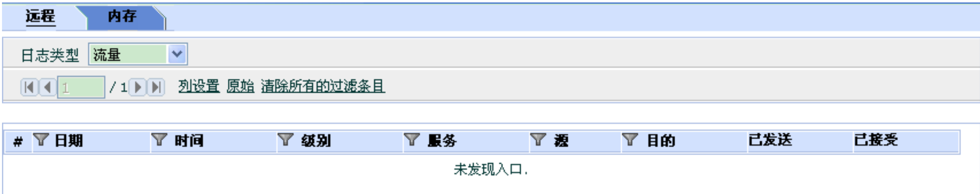


图29.8-1　查看日志信息

以下是使用基于 web 的管理器查看日志文件时使用的图标以及日志列表中栏目条的功能说明。

参数信息：

参数名称	参数说明
页面导航	点击设置进入下一页、前一页等翻页设置。
栏目设置	点击添加或删除显示的日志信息。
原始格式或设定格式	点击“原始格式”以其原始格式的日志信息显示。 点击“设定各式”以栏目格式显示日志信息。
清除所有过滤项	点击清除所有对日志文件设置的过滤项。

29.9 自定义日志信息显示

自定义日志显示可以锁定查看日志的某一部分或查看不同格式的日志信息。例如，日志信息可以以原始格式或定义的格式显示。日志信息以格式化形式显示时，您可以自定义显示栏或过滤日志信息。日志信息以原始格式显示时，日志信息便是如同在日志文件中的显示。

过滤项设置也是自定义显示日志信息的一种方法。使用过滤图标，您可以设置显示具体的日志信息。例如，您只想查看日志严重级别为警报的事件日志信息。在格式化界面显示下，您只能自定义日志信息的显示栏目与过滤项。



注意：

有关过滤日志信息的详细信息，参见“将过滤选项添加到基于 web 管理器列表”。

29.9.1 日志信息显示列设置

使用栏目设置窗口可以定义日志显示的格式。当选择“设定格式”时，显示列设置。根据您的查看要求，可以增加或删除显示的栏目或更改栏目显示顺序。在格式化界面显示下，您只能自定义日志信息的显示栏目与过滤项。

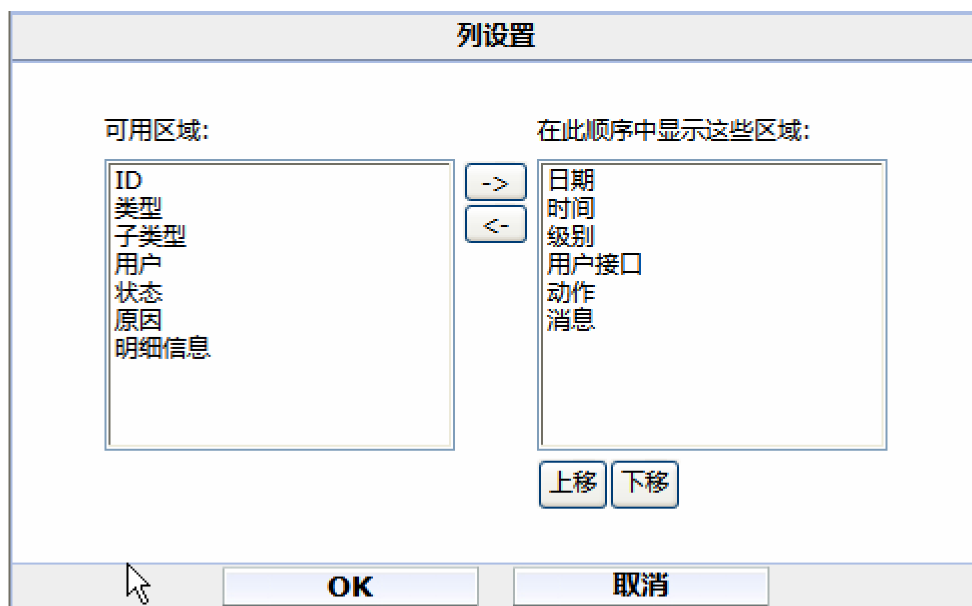


图29.9-1　设定日志信息显示格式

设定列设置信息

1. 进入日志与报告>日志访问。
2. 选择您所要访问的日志类型。
3. 选择日志所存放的位置：ZXSEC US 设备内存。
4. 点击信息栏设置图标。

5. 选择栏目名称并做以下的配置。

参数信息：

参数名称	参数说明
可选栏目	选择在日志信息显示中所要包含的说明日志信息的属性。
向右箭头	向右箭头键。从可选域中选择日志显示时所包含的信息栏目。
向左箭头	向左箭头键。从显示信息所包含的栏目中撤消某些栏目的显示。
上移	在域列表中选定一项域信息，将域向上移动一个位置顺序。
下移	在域列表中选定一项域信息，将域向下移动一个位置顺序。

6. 点击 OK 确认。



注意：

详细的栏目项信息提供了完整的原始日志条目。如果日志包含的信息在任何其它更详细的栏目中都不涵盖，则不需要使用该目录栏信息。

29.9.2 日志信息过滤

设置在大量的日志文件或许多日志信息中过滤日志内容。Web 过滤提供了在日志信息列表中查找具体日志信息的方法。

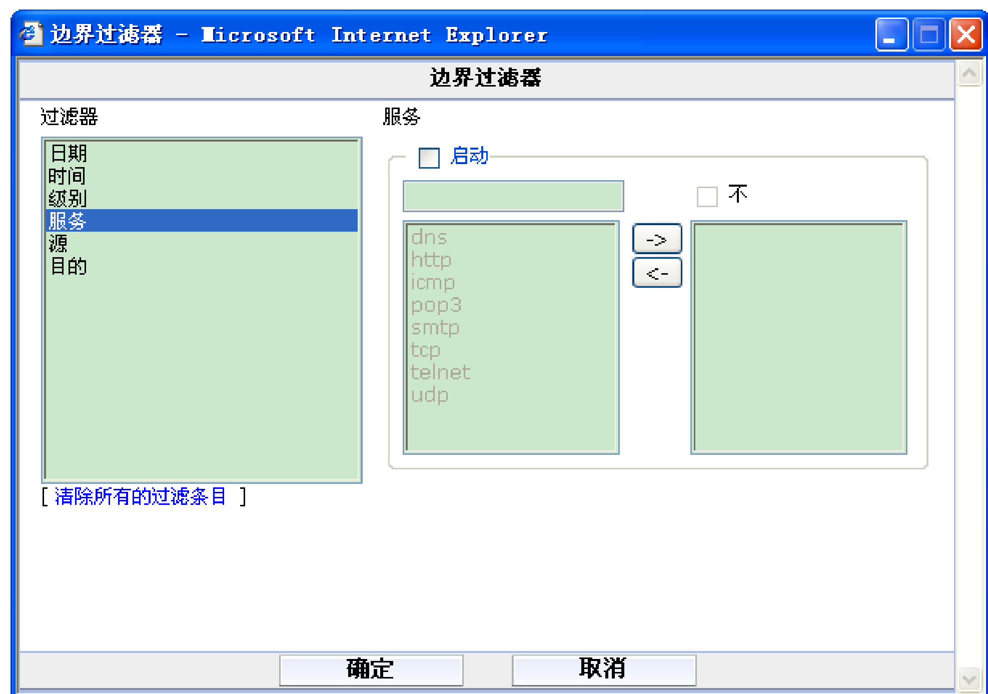


图29.9-2 日志过滤

过滤设置只有在您登录 ZXSEC US 设备时生效。当您退出时，过滤选项将不保持您登录时所设置的选项。



注意：

您必须设定的格式查看日志内容以及使用过滤项。

过滤日志信息

1. 进入日志与报告>日志访问。
2. 选择您所要访问的日志类型。
3. 从类型列表中选择日志存储的位置：US 设备内存。
4. 如果您查看 USLA 设备中的日志文件，点击查看日志文件。
5. 选项您要过滤的栏目，并点击过滤标志。
6. 在文本编辑字段输入过滤规则。

7. 选择输入的过滤规则是否与您过滤的项目符合或在规定的数据内过滤信息。

8. 如果您设置排除内容，点击“否”。过滤图标呈绿色时表示过滤项生效，反之，呈灰色时表示没有使用过滤设置。需要关闭过滤项，点击过滤图标并点击“重设过滤”。

29.10 内容存档

通过内容存档菜单，您可以从 ZXSEC US 设备基于 web 的管理器查看存档在 USLA 设备中的日志。内容存档菜单中包括四个选项栏，分别为 HTTP、FTP、Email 与 IM，您可以查看每种类型存档的日志。

查看内容存档之前，您需要在 ZXSEC US 设备中启动该功能。内容存档在保护内容表中启动。有关在保护内容表中启动内容存档的详细信息，参见“防火墙保护内容表”。

在配置内容摘要/存档时，您需要在保护内容表中启动以下选项：

- 对 HTTP 流量的反病毒配置
- HTTPS
- Web URL 过滤
- Web 过滤 HTTPS

ZXSEC US 设备只允许内存的六分之一来传输内容存档文件。例如，128RAM 的内存中只有 8MB 用于传输内容存档文件。如果配置了反病毒扫描，建议不要启动全部内容存档。



注意：

以后的软件版本中将支持 NNTP 选项。

29.10.1 配置内容存档

防火墙菜单中，可以配置与启动内容存档。内容存档只有在 ZXSEC US 设备配置启动将日志记录到 USLA 设备时可用。US Service 日志分析服务只提供内容摘要。如果您将日志记录到 US Service 日志分析服务器，USLA/US Service 下拉菜单中只有“无”或“摘要”选项。

启动 ZXSEC US 设备的内容存档功能

1. 进入“防火墙>保护内容表”。
2. 点击保护内容表旁边的编辑图标。
3. 点击蓝色的三角扩展内容存档选项。
4. 选中您需要在系统面板显示内容元信息的功能框。
5. 从下拉菜单中选择设置存档到 USLA/US Service 的设置，分别为“无”、“摘要”与“全部”。
6. 如需要，选中将垃圾邮件存档到 USLA 设备的功能框。
7. 点击 OK 确认。

如果您将日志存储在 US Service 日志分析服务器中，在设置内容存档选项中，只有“无”或“摘要”可供配置。US Service 日志分析服务只允许存档内容摘要。

29.10.2 查看内容存档

通过 ZXSEC US 设备基于 web 的管理器中的内容存档菜单，您可以查看全部存档的日志信息，以及存档在 USLA 设备或 US Service 日志分析服务器中的日志。US Service 日志分析服务器中只存储日志的内容摘要信息。

如果您需要查看原始格式的日志，点击栏目设置图标旁边的“原始格式”。有关栏目设置的详细信息，参见“栏目设置”。

查看内容存档

1. 进入“日志与报告>内容存档”。
2. 点击存档日志类型的栏目。

查看 US Service 日志分析服务器中的日志内容摘要

1. 进入“日志与报告>内容存档”。
2. 在日志设备列表中选择 US Service。
3. 点击查看日志的内容摘要。

E-mail报警

SMTP服务器：
Email来自：
发送邮件至：
认证： 启用
SMTP用户：
密码：
测试连接

以下类别发送报警邮件

间隔时间： 5 (分钟)
检测到入侵
检测到病毒
阻断Web访问
HA状态变化
检测到非法流量
防火墙认证失败
SSL VPN登陆失败
管理员登陆和退出
IPsec通道错误
L2TP/PPTP/PPPoE错误

图29.10-1 警报邮件选项

29.11 报警邮件

报警邮件功能是指 ZXSEC US 设备监控某些安全级别的日志的功能。例如，您需要获得管理员登录与退出的通知，您便可以配置在管理员登录与退出时发送报警信息。该功能可以根据日志设置的严重级别来发送报警信息。

29.11.1 配置报警邮件

配置报警邮件之前，确定您至少配置了一个 DNS 服务器。ZXSEC US 设备使用 SMTP 服务器连接到邮件服务器，并且必须在您 DNS 服务器中查找该名称。

1. 进入日志与报告>报警邮件。

2. 配置以下选项并点击“应用”生效。

参数信息：

参数名称	参数说明
启动认证	选中该功能框启动 SMTP 认证。
SMTP 服务器	SMTP 服务器的名称以及地址。
发件人	SMTP 用户名。
收件人	输入一个或最多三个邮件的接收人地址。
启动验证	选中验证功能框启动 SMTP 验证。
SMTP 用户	输入登录 SMTP 服务器发送报警邮件用户的用户名。如果您启动了 SMTP 认证选项，需要设置该选项。
密码	输入登录 SMTP 服务器发送报警邮件的密码。如果您启动了 SMTP 认证选项，需要设置该选项

3. 点击“连接测试”，在您在以上配置的邮箱中接收到测试邮件信息。

4. 您可以配置以下的情况下发送报警邮件。

参数信息：

参数名称	参数说明
间隔时间	设置报警邮件发送到收件人之前的时间间隔。
入侵检测报警	根据入侵检测发送报警邮件。
病毒检测报警	根据病毒检测发送报警邮件。
Web 访问被阻断报警	根据 web 访问阻断的情况发送报警邮件。
HA 状态更改	设置 HA 状态更改时发送报警邮件。
非法流量检测报警	设置在 ZXSEC US 设备检测到非法流量时发送报警邮件。
防火墙验证设备	设置在防火墙验证时发送报警邮件。
SSLVPN 登录失败	设置发生 SSLVPN 登录失败时发送报警邮件。
管理员登录/退出	设置在管理员登录与退出时发送报警邮件。
IPSec 通道错误	设置在 IPSec 通道配置发送错误时发送报警邮件。
L2TP/PPTP/PPPoE 错误	设置在 L2TP/PPTP/PPPoE 错误时发送报警邮件。
配置更改	设置在设备配置更改时发送报警邮件。
US Service 许可证过期（以天计）	设置在 US Service 许可证过期后发送报警邮件通知的持续时间。
磁盘使用率（百分比）	设置在磁盘使用率达到某个百分比设置时发送报警邮件。
US Service 日志磁盘配额	设置根据 US Service 日志磁盘配额的使用情况发送报警邮件。

5. 设置如果需要基于日志的严重性级别发送报警邮件。这样的配置下，ZXSEC US 设备在任何具体某项日志出现在日志文件时便发送报警邮件。

6. 在最低严重性级别列表里设置最低的严重性级别。

7. 点击“应用”。



注意：

默认的最低的日志严重性级别为“报警”。在到达所设定的时间间隔之前如果收集到不止一条的日志信息，这些日志信息将集中在一封报警邮件邮件中并发送。

29.12 报告

USLA 设备的报告功能被集成在 ZXSEC US 设备。通过日志与报告菜单，您可以配置生成 USLA 报告、查看报告与打印报告。您甚至可以查看存储在 USLA 设备中的日志内容存档。

通过日志与报告菜单，您可以配置基本的流量报告。基本流量报告使用存储在 ZXSEC US 设备内存中的日志信息以图表的格式显现基本的流量信息。

29.12.1 基本流量报告

ZXSEC US 设备利用收集到的流量信息生成以图示显示的每项服务的使用情况。图中显示每项服务的流量情况。

进入日志与报告>报告，并从“数据源列表”中选择“内存”查看日志报告。

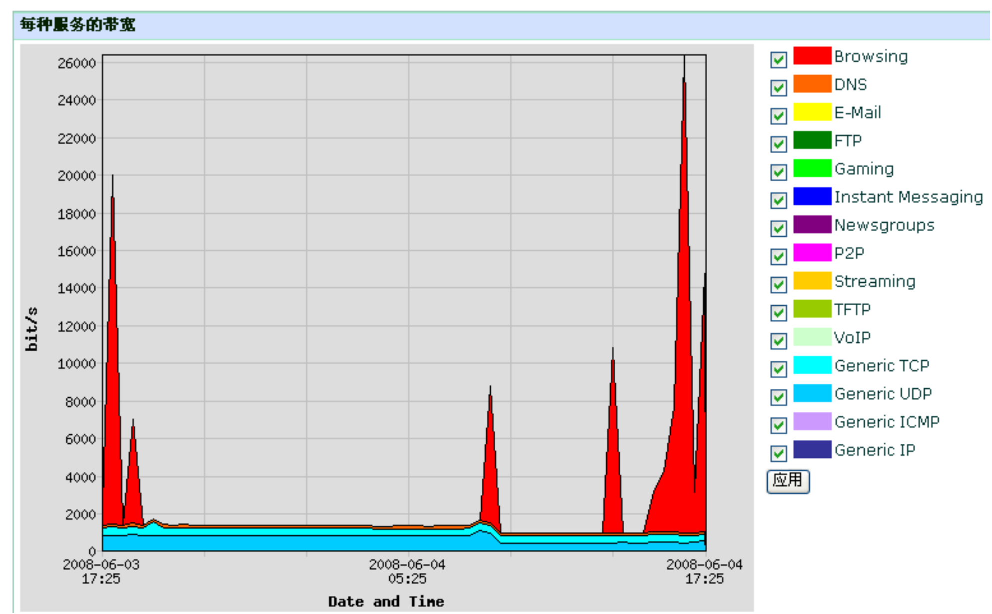


图29.12-1 每项服务占用的带宽

参数信息：

参数名称	参数说明
时间间隔	设置所要查看日志的时间段。您可以设置查看一天、三天、一个周或一个月。默认的设置是一天。当您刷新浏览器或进入其它菜单时，恢复为默认的设置。
服务	默认的情况下显示所有的服务。当您刷新浏览器或进入其它菜单时，恢复为默认的设置。查看服务选项栏，设置图表中显示的服务。 ● 浏览 ● 即时通讯 ● DNS ● 新闻组 ● 邮件 ● P2P ● FTP ● 流媒体 ● 游戏 ● TFTP ● 常规 UDP ● VoIP ● 常规 ICMP ● 常规 TCP ● 常规 IP

报告不是实时更新的。您可以进入日志与报告>报告，刷新报告显示。



注意：

用于生成该报告的信息是存储在 ZXSEC US 设备内存中的日志信息。当 ZXSEC US 设备重新设置或重新启动时，所有的日志信息都将丢失。

29.12.2 配置报告显示图

ZXSEC US 设备生成的报告以图表的形式显示了一定范围协议的使用情况。例如，您只可以查看最近三天中邮件服务流量的情况。

更改图示信息

1. 进入日志与报告>报告。
2. 设置“时间间隔”。
3. 点击选择您要查看的服务并点击“应用”。

根据您所选择查看的内容，图表进行刷新显示。最大占用带宽的协议将不改变。



注意：

该图表显示是比较简单的报告。如果您需要更为详细的报告，USLA 设备可以生成 140 多种不同的报告，提供更加详细并具体的报告内容。